# Chapter One
# Introduction

In this thesis, I examine how (i) economic, (ii) legal, (iii) cultural, (iv) political and (v) social factors, along with (vi) 'mainlandisation' shape the nature of Internet crimes, especially Internet banking crime, and how these crimes are investigated in Hong Kong. To achieve this, I examine how organisations such as banks and the police work with the prosecuting authorities to process this type of crime.

Due to the global nature of the Internet, Internet banking fraud now occurs in countries all over the world. As different societies have distinct policing traditions and social-economic and political backgrounds, individual countries are likely to police and regulate Internet banking fraud differently. For example, the Chinese government monitors and regulates the Internet in a highly restrictive manner, by enacting tough legal and administrative regulations. In addition to having enacted sixty Internet regulations over the last 20 years, the Chinese government uses the People's Liberation Army (PLA), the state police and state censorship systems to police Internet use. Internet regulations in China are also enforced by the provincial branches of state-owned organisations, ISPs and businesses (both private and state owned). This heavy policing of the Internet reflects the fact that China is a communist country with a long history of state-controlled and state-centred policing, where the police have traditionally been used to help build the socialist state by protecting the economy and the Communist Party leadership. Even though China has changed politically since the enactment of the 1978 open-door policy, the police still have the task of

upholding "socialism with Chinese characteristics". To this end, the old policing structures have been adapted to meet new challenges, including the criminal use of the Internet. Because the police are a part of, and are recruited from within society, their competence in dealing with, and attitude towards technology-related and economic crimes reflect the nature of that society.

Although Hong Kong is now part of the People's Republic of China (PRC), as a capitalist enclave it has a very different history. Nonetheless, the Hong Kong police force is also an arm of the government and is able to quickly respond to governmental priorities. The Hong Kong government has also introduced a number of laws and regulations to deal with Internet and economic crime. However, the law and the police operate very differently on this side of the border. As I shall argue, the government also seeks to ensure that Hong Kong's laws, regulations and police protect the region's reputation as a financial centre, taking a hard line on any activity which threatens this. However, the question remains as to how the handling of Internet economic crime differs in Hong Kong and how the Hong Kong authorities police cross-border Internet fraud or Internet economic crimes.

Definition of Internet Banking Fraud

Traditionally, fraud is seen as a white collar crime committed by people in positions of power or professional occupations, such as accountants, bank managers and corporate executives, i.e. those who wear a 'white collar' at work.[1] However, there is no one specific type of white collar crime, as the genre can

[1] See Sutherland, E.H. (1940) 'White-collar Criminality', American Sociological Review, Vol. 5, pp. 1-12.

include acts such as altering records, industrial espionage and economic crimes such as fraud and embezzlement. In recent years, white collar crime has also come to include Internet crime or 'cyber-fraud', such as Internet banking fraud, which is an evolving global occurrence. Potentially, anyone or any business can be affected by this type of fraud. Even so, it is difficult to define what actually constitutes Internet banking fraud, especially given the rapid development of Internet technology over the last two decades. For example, Internet banking fraud can now be committed by a self-taught computer user at home in addition to the fraud committed by highly trained white collar professionals in an office setting.

Wall has categorised Internet crime into the following three groups:
"

*(i) Computer integrity crime: - [includes] hacking, cracking, vandalism, spying, denial of service, the planting and use of viruses and Trojans;*

*(ii) Computer-assisted (or related) crimes:- uses networked computers [Internet] to commits crimes to acquire money, goods or services dishonestly [such as phishing, advance fee frauds, theft];*

*(iii) Computer content crimes: - related to the illegal content on networked computer systems and include trade and distribution of pornographic materials as well as the dissemination of hate crime materials."*[2]

Broadhurst's definition of Internet crime includes the following:

*"Conventional crimes in which computers are instrumental to the offence,*

- *such as child pornography and intellectual property theft; attacks on computer networks; and conventional criminal cases in which evidence exists in digital form.*

[2] Wall, S.D. (2007) Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity, pp. 49-50. Also, see Wall, S.D. (2010) Criminalising cyberspace: The rise of the Internet as a 'crime problem', in Jewkes, Y. Yar, M. (eds.), Handbook of Internet Crime, Cullompton: Willan Publishing, p. 99.

- *Interference with lawful use of a computer: cyber-vandalism and terrorism;denial of service; insertion of viruses, worms and other malicious code.*

- *Dissemination of offensive materials: pornography/child pornography; on-linegaming/betting; racist content; treasonous or sacrilegious content.*

- *Threatening Communications: extortion; cyber-stalking.*

- *Forgery/counterfeiting: ID theft; IP offences; software, CD, DVD piracy;copyright breaches etc.*

- *Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g. virtual 'snake oils'); on-line securities fraud; and*

- *Other: Illegal interception of communications; commercial/corporate espionage; communications in furtherance of criminal conspiracies; electronic money laundering*."[3]

In this thesis, I examine Internet-based economic crimes including Internet banking fraud. Internet fraud is best described as a crime committed by a person who uses Internet technology to illegally pursue financial gain[4]. Article 8 of the Council of Europe Convention on Cybercrime defines computer-related fraud as:

> *a) any input, alteration, deletion or suppression of computer data, [or]*
> b) *any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*[5]

As Smith writes:

> *"…most economic crimes involving fraud or dishonesty that have been perpetrated in recent years have involved*

[3] Broadhurst, R.G. 2006, 'Developments in the global law enforcement of cyber-crime', *Policing*: *an International Journal of Police Strategies and Management*, Vol. 29(3): 408-433
[4] Or sometime none-financial gain.
[5] Council of Europe, Convention on Cybercrime, Budapest, 23.XI. 2001,

> *the use of computers and the Internet, simply because modern businesses rely so heavily on digital technologies for accounting purposes and for transfer of funds. Many identity-related crimes are facilitated through the use of the Internet, which provides a rich source of personal information that can be stolen and misused. The vast majority of such crimes seek to extract money from victims through acts of dishonesty, making them fall within the definition of fraud*."[6]

Accordingly, it is difficult to define Internet banking fraud as a single, separate and distinctive type of crime. In this thesis, I use the definition of Internet fraud included in the Hong Kong statutes:

> *"A person commits internet banking fraud if he obtains access to an online banking account via a computer to carry out any banking activities, with an intent to commit an offence; or with a dishonest intent to deceive, with a view to dishonestly gaining advantage for himself or another; or with a dishonest intent to cause loss to another*." [7]

Incidence

According to Wong,[8] in 1996, "*the first year computer crime records were kept, there were only 21 cases of computer crime, 4 involving hacking, 6 the publication of obscene articles, 4 the criminal damage of data and 7 others for a total of 21. This was increased to 34 cases in 1998, and 317 in 1999 (238 involving hacking, 32 the publication of obscene articles, 4 the criminal damage of data, 18 internet fraud and 25 others)*". Wong provides the following table of reported computer crimes:

[6] Smith, R. G. (2010), Identity theft and fraud, in Jewkes, Y. Yar, M. (eds.), Handbook of Internet Crime, Cullompton: Willan Publishing, p. 275.
[7] See Computer Crimes Ordinance 1993.
[8] See Wong K.C. (2005) 'Computer Crime and Control in Hong Kong'. Pacific Rim Law & Policy Journal, Vol. 14, No. 2.

**Table 1.1: Reported Computer Related Crimes: 1996-1999**

| Case Name | 1996 | 1997 | 1998 | 1999 |
|---|---|---|---|---|
| Hacking | 4 | 7 | 13 | 238 |
| Publication of obscene articles | 6 | 6 | 13 | 32 |
| Criminal damage of data | 4 | 3 | 3 | 4 |
| Internet shopping fraud | 0 | 2 | 1 | 18 |
| Others | 7 | 2 | 4 | 25 |
| Total | 21 | 20 | 34 | 317 |

*Source: Legislative Council Panel on Security, "Computer Related Crime" LC Paper No. CB2 1187/99-00(04) (2 March 2000).*

As Table 1.2 shows, reported computer-related crime rose steadily between 1996 and 2004, increasing from 21 cases in 1996 to 588 cases in 2003, an increase of 2700%. The biggest rise was between 1998 and 1999, when the growth rate was 832%. In 2001, the number of reported computer crimes decreased slightly to 235 cases.

According to the statistics of the Hong Kong police, the property losses attributed to Internet crime were HK$3 million in 2000, rising to HK$17 million 2011 while the total number of computer cases rose from 34 in 1998 to 368 in 2000.[9]

Wong's research also shows that the number of reported computer-related crimes increased between 1996 and 2004.[10]

[9] Ibid.

**Table 1.2: Reported Computer Related Crimes: 1996-2004**

| Computer Crime | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 (Jan – June) |
|---|---|---|---|---|---|---|---|---|---|
| Total | 21 | 20 | 34 | 317 | 368 | 235 | 272 | 588 | 280 |

*Source: Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)*

However, the actual figures for reported Internet fraud in Hong Kong are low compared to those for other crimes. As Table 1.3 shows, the number of reported cases of Internet-related theft or fraud (including banking fraud) increased between 1999 and 2006. This may have been due to better reporting and recording, greater awareness of the area and better detection. However, the crime rate may have also simply gone up:

**Table 1.3: The Number of Reported Cases of Internet-related Theft or Fraud (including banking fraud) in Hong Kong, 1999-2006**

| | **1999** | **2000** | **2001** | **2002** | **2003** | **2004** | **2005** | **2006** |
|---|---|---|---|---|---|---|---|---|
| E-fraud [e-banking-related] | 57 | 49 | 36 [8] | [6] | [8] | [19] | [3] | [0] |
| E-deception | 18 | 29 | 65 | 54 | 103 | 120 | 154 | 205 |
| Total | 75 | 78 | 101 | 60 | 111 | 139 | 157 | 205 |

(Sources: The Hong Kong Police, Technology Crime Division, 2007, Lau, L.Y.C. 2005) [11]

This increase coincided with the November 1999 establishment of a specialist computer crime team within the Department of Justice dedicated to prosecuting Internet-related crimes.[12]

[10] Wong K.C. (2005) Ibid.

[11] The Hong Kong Police [online]. Available from: <http://www.police.gov.hk/hkp-home/english/tcd/overview.htm>, see also Lau, Y.C.L. (2005) 'Governance in the Digital Age: Policing the Internet in Hong Kong', in Broadhurst, R. Grabosky, P. (eds.) Cyber-Crime: The Challenge in Asia. Hong Kong: Hong Kong University Press, p. 93, Table 5.1.

Nonetheless, despite this rise, the figures are low compared with those for traditional crimes, such as traditional theft (see Table 1.4 below):

**Table 1.4: The Number of Traditional Crime and Theft Cases in Hong Kong, 1999-2006**

| Years | **1999** | **2000** | **2001** | **2002** | **2003** | **2004** | **2005** | **2006** |
|---|---|---|---|---|---|---|---|---|
| Overall crime | 76771 | 77245 | 73008 | 75877 | 88377 | 81315 | 77437 | 81125 |
| All theft, including:<br>a) Missing motor vehicle<br>b) Snatching<br>c) Pick-pocketing<br>d) Shop theft<br>e) Other theft | - | - | 29542 | 32025 | 40887 | 37500 | 35213 | 37089 |

(Source: The Hong Kong Police)[13]

Similarly, there have been far fewer prosecutions and convictions for Internet fraud than for traditional crimes. The Department of Justice did not begin publishing the figures for Internet-related crime[14] until 2002 (Table 1.5), partially because the specialist computer crime unit was only set up in 1999.

**Table 1.5: The Number of Prosecutions and Convictions (Internet-related Crime, including fraud) in Hong Kong, 2002-2006**

| Years | **1999** | **2000** | **2001** | **2002** | **2003** | **2004** | **2005** | **2006** |
|---|---|---|---|---|---|---|---|---|
| No. Cases Prosecuted | - | - | - | 12 | 10 | 15 | 17 | 15 |
| No. People Convicted | - | - | - | 12 | 8 | 18 | 15 | 11 |

(Source: The Department of Justice, Hong Kong, Yearly Review from 1999-2006)

Comparing Tables 1.3 and 1.5, it seems that the overall number of prosecutions has remained low, i.e. less than 20 cases in any one year, even though the number

[12] See The Department of Justice, Hong Kong, Yearly Review 1999 and 2000.
[13] The Hong Kong Police. [online]. Available from: < http://www.police.gov.hk/hkp-home/english/statistics/index.htm>.
[14] See the Department of Justice, Yearly Review from 1999-2001. However, the 2001 yearly review mentions that there was an increase of 13.4% in the number of personal computers affected by computer attacks and 334 cases of computer crime were reported to the police.

of reported Internet crimes has increased significantly. For example, while 205 crimes were reported in 2006, only 15 cases were prosecuted, i.e. 7.32%, despite the fact that the dedicated team of computer crime prosecutors had been operating since 1999. There may be a number of reasons for this discrepancy, including the fact that the electronic evidence needed to prove an offender's criminal intent may have been lacking. According to Smith et al.,[15] almost 14% of the computer crime cases in the US fall within this category, with the prosecutor stopping the prosecution due to a lack of proof of the offender's criminal intent (*mens rea*). Another reason may be that the prosecutor has insufficient electronic evidence (both as to *mens rea* and *actus reas*) to prove that the offender is guilty beyond reasonable doubt. Smith et al.[16] point out that over 17% of the computer crime cases in the US fall within this bracket, where the prosecutor has dropped the prosecution. Another reason may be the fact that in some cases the majority of the electronic evidence is located outside Hong Kong, which makes it difficult for the police to access and obtain. According to Walden,[17] mutual legal assistance (MLA) procedures tend to be notoriously slow and bureaucratic. Therefore, by the time the police have obtained the required electronic evidence its evidential weight may have dropped considerably, rendering the usefulness of the evidence questionable in court.

[15] Smith, R.G. Grabosky, P. Urbas, G. (2004) Cyber Criminals on Trial. Cambridge: Cambridge University Press, p. 39.
[16] Ibid. Smith et al. also point out that there are many other reasons why US prosecutors drop prosecutions, including the fact that the suspect is to be prosecuted by another authority (11.73 per cent), no federal offence evident (10.71 per cent), minimal federal interest or no deterrent value (10.71 per cent), no known suspect (8.67 per cent), juvenile suspect (5.10 per cent), agency request (5.10 per cent), civil, administrative, or other disciplinary alternatives (3.06 per cent), office policy (fails to meet prosecutorial guidelines) (3.06 per cent), jurisdiction or venue problems (2.55 per cent), pre-trial diversion completed (2.55 per cent), lack of investigative or prosecutorial resources (2.04 per cent), witness problems (1.53 per cent), suspect being prosecuted on other charges (1.53 per cent), and other (unspecified reasons) (6.63 per cent).
[17] Walden, I. (2007) Computer Crimes and Digital Investigations. Oxford: Oxford University Press, para. 5.81, p. 322.

The Hong Kong police released figures on technological crimes in 2010,[18] which showed that cybercrime had increased sharply by 39 per cent from the previous year. A total of 840 cases of Internet crime were reported to the police in 2010, of which 293 involved commercial Internet fraud, including Internet banking fraud, corresponding to an increase of 54 per cent over the same period in 2009.

Furthermore, the number of reported cases of Internet-related theft or fraud (including banking fraud) increased from 75 in 1999 to 205 in 2006. This rise coincides with the establishment of the specialist prosecuting unit for Internet-related crimes within the Department of Justice in November 1999.[19] Despite the increase, the figures for reported Internet fraud in Hong Kong are low compared with those for traditional crime, such as theft, which rose from 29542 in 2001 to 37089 in 2006.

There are also far fewer prosecutions and convictions for Internet fraud than for traditional crimes. The figures for Internet-related crime (which were not published until 2002) show that only 12 cases resulted in conviction in 2002 and the number only rose to 15 in 2006.[20]

Although the rates of Internet fraud are lower than the rates for other crimes, this does not mean that these crimes are less damaging. Wong's research provides some idea of the financial effects of computer crime in Hong Kong. His figures

[18] The Standard News Paper, (August 16, 2010) Interpol chiefs for city summit as Cybercrime soars, Hong Kong.
[19] See The Department of Justice, Hong Kong, Yearly Review 1999 and 2000.
[20] See the Department of Justice, Yearly Review from 1999-2001. However, the 2001 yearly review mentions that there was an increase of 13.4 per cent in the number of personal computers affected by computer attacks and 334 cases of computer crime were reported to the police.

show that the overall cost of Internet crime rose from HK$7,643.737 in 2001 to HK$19,186.201 in 2003. He also points out that based on figures from the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) on virus attacks and hacking between 2000 and 2003, the 'dark figures' on unreported computer crime, and hence unreported costs are likely to be large.[21]

The Global Context

As Hong Kong is not the only city state that experiences Internet fraud, it must liaise with other international bodies to investigate crimes and pursue offenders. However, as I argue in this thesis, each country polices the Internet differently within its national borders. Nonetheless, in recent years, some co-ordinated efforts have been made to align the global strategies for policing the Internet, including the establishment of international organisations to fight internet crime. While some of these organisations are publicly funded, others are commercially funded by privately owned corporations. For example, the UK-based International Cyber Security Protection Alliance (ICSPA)[22] was established in 2011 by a group of large national and multi-national corporations to provide extra resources and support for law enforcement agencies fighting cybercrime. Europol is a member of this alliance. However, the International Criminal Police Organisation[23] (Interpol), which is mostly funded by the membership fees from its 190 member states, is by far the biggest and best established international organisation for policing Internet crime. Hong Kong is a member of Interpol, and

[21] Wong K.C. (2005) Ibid.
[22] See International Cyber Security Protection Alliance, [Online] [cited 31/12/2011], at: <https://www.icspa.org/home/>.
[23] See International Criminal Police Organisation, [Online] [cited 31/12/2011], at: < http://www.interpol.int/About-INTERPOL/History>.

in 2010, 188 Interpol member states met in Hong Kong to discuss the increase in technological crime, indicating the important role that Hong Kong now plays in the policing of the Internet. Moreover, as discussed in Chapter Eight, the Hong Kong police regularly liaise with and assist authorities in mainland China in the investigation of Internet crimes, including Internet banking fraud.

However, any co-ordinated global response to Internet crime has to contend with the fact that the legal systems in different societies largely reflect each society's particular economic, social, cultural and political environment. In this thesis, I investigate how the phenomenon of Internet crime is handled by the banks, police and courts in Hong Kong and how this reflects Hong Kong's social, political, legal and economic environment and its traditions and values.

Mainlandisation

One of the primary factors influencing the way Hong Kong's banks, police and courts handle Internet banking crimes is the process of 'mainlandisation', which refers to the re-alignment of Hong Kong's political, economic and legal systems with the motherland following its reintegration with China in 1997. In addition to affecting the policing of Internet crime, the process of mainlandisation has influenced the nature of the crime itself, which often involves trans-border economic activities.

As Lo states, "*Hong Kong has experienced a process of mainlandization of its political, economic and legal systems.*"[24] He defines mainlandisation as:

> *"[The] policy of making Hong Kong politically more dependent on Beijing, economically more reliant on the Mainland's support, socially more patriotic toward the motherland, and legally more reliant on the interpretation of the Basic Law by the PRC National People's Congress*."[25]

In this thesis, I follow Lo's definition of mainlandisation and argue that closer integration has increased the opportunities to use the Internet to commit offences connected to banks, victims and perpetrators in the mainland. Mainlandisation has also affected the policing of the Internet, raising questions about Hong Kong law enforcement agencies' ability to reach perpetrators in the mainland.

Hong Kong's integration with mainland China accelerated in the late 1990s, after Hong Kong experienced a series of economic and social crises including the Asian financial crisis in 1997, the spread of the avian flu and the outbreak of severe acute respiratory syndrome (SARS).[26] Due to the compounding nature of the crises, the Hong Kong government actively sought help from the mainland and pushed for greater economic integration. It was also in Beijing's interest to help Hong Kong, as politically it would not have been acceptable for Hong Kong to experience economic and political failure only a few years after reintegration. These factors helped accelerate the pace of Hong Kong's integration with the mainland.

---

[24] T. Wing Lo. (2012) 'Resistance to the Mainlandization of Criminal Justice Practices: A barrier to the Development of Restorative Justice in Hong Kong'. International Journal of Offender Therapy and Comparative Criminology, 56(4), p. 632.
[25] T. Wing Lo. Ibid.
[26] Kui-Wai Li, (2012) Op Cit.: p. 2. See also Lau Siu-kai, (2000) Government and Political Change in the Hong Kong Special Administration Region, in James C. Hsiung, (ed.) Hong Kong the Super Paradox: Life after Return to China. Houndmills: MacMillan, pp. 35-57.

Hong Kong has undoubtedly had a long and close trading and commercial relationship with mainland China. Hong Kong's re-exports to the mainland increased substantially from HK$705.8 billion in 2003 to HK$1,831.7 billion in 2012, representing an average annual growth of 11.2 per cent over the period, with average annual growth rates of 23.6 per cent. In the past decade, the mainland has been the largest importer of Hong Kong's re-exports and the main supplier of its imports, accounting for 49.8 per cent and 45.7 per cent, on average, of Hong Kong's total re-exports and imports, respectively. In 2005, mainland China replaced the US as the largest importer of Hong Kong's domestic exports, accounting for an average of 36 per cent of total domestic exports over the last decade. Hong Kong has also played an important role in the external trade of mainland China in recent years. According to the trade statistics of China Customs, Hong Kong was the mainland's second largest trading partner in 2012. In that year, mainland China's imports from Hong Kong amounted to US$18.0 billion, while its exports to Hong Kong were US$323.5 billion.[27] Moreover, since the onset of the economic reforms, increasing numbers of tourists from the mainland have been permitted to visit Hong Kong. According to the Hong Kong Tourism Commission, mainland China continues to be Hong Kong's largest source of visitors, with the 34.9 million people who visited in 2012 (up 24.2 per cent from 2011) accounting for 71.8 per cent of Hong Kong's total arrivals.[28] However, the increased presence of mainland Chinese in Hong Kong has

[27] See Hong Kong Government, Census and Statistics Department, website: < ,http://www.censtatd.gov.hk/hkstat/sub/sp230.jsp?productCode=FA100252> [Visited 22/6/2013].
[28] See Hong Kong Tourism Commission. Website: <http://www.tourism.gov.hk/english/statistics/statistics_perform.html>, [Visited 12/7/2013].

triggered some hostility towards mainland China feelings, and leading to fears that Hong Kong's core values and identity are being undermined.[29]

Another example of Hong Kong's deepening economic integration with mainland China is the free trade agreement that Hong Kong and China signed in 2003, shortly after the SARS crisis. The Closer Economic Partnership Arrangement (CEPA) between mainland China and Hong Kong has three clear objectives: i) to progressively reduce or eliminate tariffs and non-tariff barriers on all trade in goods; ii) to liberalise the trade in services through the reduction or elimination of all discriminatory measures, especially the mainland government's duties and taxes; and iii) the promotion of mutual trade and investment. Under CEPA, Hong Kong registered companies and their products enjoy preferential access to the mainland domestic market. Many of the trade preferences in the CEPA agreement go beyond the concessions that China made to the World Trade Organisation (WTO). As a result, in theory, Hong Kong immediately gained access to mainland China's 1.3 billion domestic consumers. Moreover, year on year, the Chinese domestic consumer market has expanded by an average of 14.9% per annum since 2000.[30]

However, due to China's weak legal system, the mainland's large domestic consumer market has also attracted numerous informal economic activities or 'dark market' practices, such as corruption, bribery and business kickbacks. In

[2929] See Jones, C.A.G. 'Looking North', Journal of Taiwan in Comparative Perspective Vol. 3 December 2010.
[30] See China Daily 'Year-ender: Domestic consumption in 2012' website < http://www.chinadaily.com.cn/bizchina/2013-01/14/content_16113942.htm>, [Visited 21/3/2013].

2012, China was ranked 80th out of 176 countries on the Transparency International Corruption Perception Index.[31] As reported by CNN:

> "*China has become the world's second largest economy, doing business in China is now perceived to be more corrupt. [As] the world's leading economies should lead by example, making sure that their institutions are fully transparent and their leaders are held accountable. This is crucial since their institutions play a significant role in preventing corruption from flourishing globally…* "[32]

One question for this thesis is what this means for the level of cross-border Internet banking fraud? Accordingly, in this thesis, I will also examine how do closer economic integration and mainlandisation have affected the ways in which Internet banking fraud is handled by the banks and the criminal justice system?

Fears for the Erosion of the Rule of Law

The rule of law is said to be one of Hong Kong's key core values. Since Hong Kong's reintegration with China in 1997, there have been fears that the rule of law in Hong Kong is under threat. According to Lo,[33] in China "power is everything". He goes on to state that, "*The abuse of power and official positions state functionaries prevailed…bribery, [kickback] and obstruction of justice are the most common form of corruption at all levels of the political hierarchy [in China]…*".[34] Consequently, many in Hong Kong fear that the ways in which things are done in mainland China (corruption, nepotism, gangsterism and the use of power and connections to avoid the law) will have a negative effect on Hong Kong society.

---

[31] See 2012 Corruption Perception Index, Transparency International. Website: < http://www.transparency.org/cpi2012/>. [Visited 20/3/2013].
[32] See Kevin Voigt (December 6, 2012) 'Best, worst nation for corruption'. CNN News. Website: < http://edition.cnn.com/2012/12/06/business/best-worst-corrupt-countries>. [Visited 20/3/2013].
[33] T. Wing Lo, (1993) Op Cit.: p. 46.
[34] Ibid.

According to Cullen, quoting Dicey, Bo Li and Kleinfeld-Belton, the rule of law consists of the following properties:

1. No person is to be punished other than for a breach of a properly established law, the breach of which has to be demonstrated at a hearing before the ordinary courts of the land.
2. No person is above or beyond the law regardless of their rank and no persons are to be exempted from a duty to obey the law which governs the citizens of the realm.
3. The rule of law places limits on the arbitrary or abusive use of power by government.
4. Equality before the law, so that 'everyman', whatever his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of ordinary tribunals.
5. Due process or a formal rational legal system.
6. Law and order.
7. Predictable and efficient rulings.
8. Human rights.[35]

Lo states that the principle of the rule of law, "*means that governmental authority is legitimately exercised only in accordance with written, publicly disclosed legal codes that are adopted and enforced in accordance with established procedures*".[36] These principles and procedures are intended to protect against arbitrary rule and safeguard the interests and rights of all individuals. No one is supposed to be above the law.[37]

Skolnick also argues that "*the central element of 'rule of law' is the reduction of arbitrariness by officials*".[38] He goes on to state that:

> "*... the 'rule of law' is used as the instrument of social order [crime control, but] must meet stringent tests of specificity and clarity, may act only prospectively, and must be strictly construed in favor of the accused [however, these stringent tests might be applied in*

[35] See Cullen, R (July 2005) The Rule of Law in Hong Kong. Hong Kong: Civic Exchange.
[36] Lo, T. Wing, (2012) 'Resistance to the Mainlandization of Criminal Justice Practices: A barrier to the Development of Restorative Justice in Hong Kong'. International Journal of Offender Therapy and Comparative Criminology, 56(4), p.630.
[37] See Neumann, M. (2002). The rule of law: Politicizing ethics, Aldershot:Ashgate, pp. 23-50.
[38] Skolnick, J. H. (1994) (Third Edition) Justice without trial: Law Enforcement in Democratic Society. New York: Maxwell Macmillan, p. 8.

> *various levels of strictness from one jurisdiction to another and/or from one country to another]… [The due process side of rule of law] commands that the legal standard be applied to the individual with scrupulous fairness in order to minimize the chances of convicting the innocent, protect against abuse of official power, and generate an atmosphere of impartial justice. [As a result] a complex network of procedural requirements embodied variously in constitutional, statutory, or judge-made law is imposed upon the criminal adjudicatory process-public trial, unbiased tribunal, legal representation, open hearing, confrontation, and related concomitants of procedural justice.*"[39]

The official message on the Hong Kong government website is that everyone is, *"equal before the law. It is fundamental that all persons, regardless of race, rank, politics or religion, are subject to the laws of the land*".[40] According to the government, if Hong Kong has a defining ideology, it is the rule of law, as it constitutes:

> "*… one of Hong Kong's greatest strengths. It is the cornerstone of Hong Kong's success as a leading international commercial and financial centre, providing a secure environment for individuals and organizations and a level playing field for business, [by upholding the rule of law] everyone in Hong Kong is equal before the law.*"[41]

Apart from these liberal principles, another argument that finds favour in Hong Kong is that the rule of law provides the certainty that is essential to capitalist society. Commerce needs to be sure that contracts can be relied upon, that the law

[39] Ibid.
[40] See Department of Justice, Hong Kong Government Official Website, <http://www.doj.gov.hk/eng/legal/index.html>, [Visited 21/4/2013].
[41] See Hong Kong Government Official Website, explaining the importance on Rule of Law <http://www.info.gov.hk/info/sar5/elaw_1.htm> [Visited 3/4/2013].

will guarantee that contracts will be fulfilled or enforced.[42] Kui-Wai Li, argues that:

> "*The rule of law is often regarded as a yardstick in a free economy. More importantly, the legal profession provides arbitration or service that helps to settle an activity that would have absolute outcome of win or lose between the two parties in a law suit*."[43]

The rule of law has become central to Hong Kong's reputation as a 'clean' and safe city in which to do business. This reputation is the result of Hong Kong's colonial past. According to Lo, in the 1980s, the colonial administration:

> *"…tackled corruption head on by prosecuting the wrongdoer both in the private and public sectors … The punishment of some senior Chinese officials and white expatriates demonstrated that the ICAC [and the colonial government] did not only catch small fry [and also big fish too], and that everybody was equal before the law irrespective of position, nationality or class.*"[44]

These actions convinced the Hong Kong public that the colonial administration was serious about the rule of law, as they showed that the government and its officers were subject to the law. Gradually, people in Hong Kong came to believe in the ideology of the rule of law. Accordingly, it has become increasingly common for the public to express their outrage by protesting cases in which the principle of the rule of law has been breached, especially since the 1997 hand-over. For instance, in late 1998, 'Cheung Tse-keung' was prosecuted, tried and executed in China under mainland criminal law for crimes perpetrated in Hong Kong. This 'Big Spender' case indicated a strong liaison between the Hong Kong

[42] McBarnet, D.J. (1981) Conviction: Law, the State and the Construction of Justice. London: MacMillan, p. 162.
[43] See Kui-Wai Li, who made similar comments as McBarnet. Kui-Wai Li, (2012) Economic Freedom: Lessons of Hong Kong, World Scientific Publishing: Singapore, p. 2 and p. 73.
[44] T. Wing Lo, (1993) Corruption and Politics in Hong Kong and China. Buckingham: Open University Press, p. 103.

and mainland China police. The case worried people in Hong Kong because Cheung, a Hong Kong resident, was executed for crimes committed in Hong Kong. The Hong Kong government was criticised for failing to bring Cheung back to Hong Kong to stand trial. This case was controversial because the mainland legal system is seen as arbitrary and lacking in transparency and due process. Cheung's prosecution gave rise to the fear that this was a sign of things to come, and that Hong Kong people caught in China should not expect help from their government.

Another controversial case around this time involved Sally Aw Sian, who was a very close family friend of the first Chief Executive of Hong Kong, Tung Chee Hwa. In 1999, Aw was a politically powerful and well-connected tycoon, as she was a local deputy of the Chinese People's Consultative Conference and the owner of the Sing Tao Group. At the time, the Sing Tao Group published the Hong Kong Standard, a local English language newspaper. Aw was alleged to have falsified the newspaper's circulation figures to boost its advertising income and evidence existed that she was fully aware of this fraudulent practice. Nonetheless, in February 1999, the Secretary for Justice, speaking at the Legislative Council Panel on the Administration of Justice and Legal Services, argued that Aw should not be prosecuted based on a lack of evidence and that it would not be in the public interest, because prosecution might harm the company and result in job losses. However, her three co-conspirators were found guilty based on the same evidence and sentenced to prison.

Another controversial case involved the son of a High Court judge. In December 2000, the judge's son was caught in possession of an illegal drug [ecstasy tablets] at a party. However, the prosecution decided not to offer any evidence at the trial, stating that it would not serve the interests of justice and that a conviction would adversely affect the defendant's future.

A further controversial case occurred in 2010 and also involved a relative of a prominent judge. The defendant in this case was the niece of a Final Court of Appeal judge. She appeared in the magistrate's court for failing to take a breathalyser test after being involved in a traffic accident and for slapping a police officer. She was charged with assaulting a police officer, which she admitted. A conviction for this crime would normally result in a jail sentence and a fine. However, the magistrate did not impose a custodial sentence and the judge's niece received a very lenient sentence of supervision by a probation officer. Although the case was reviewed by the Hong Kong magistracy after public outcry, the decision not to impose a custodial sentence was upheld. As Dobinson stated, "*both the [Aw] and [the judge's son] cases were extremely controversial ... to put it mildly these cases may be undermining Hong Kong rule of law ...*"[45]

According to Lo,[46] despite not being democratic in the sense of having direct elections, Hong Kong has successfully maintained the rule of law. When the citizens know they have no democracy, the rule of law becomes a most valuable

[45] See Dobinson, I. International Society for the Reform of Criminal Law, website: <http://www.isrcl.org/Papers/Dobinson.pdf>, [Visited 21/4/2013].
[46] Lo, T. Wing, (2012) Op Cit.: p. 631.

asset.[47] Accordingly, in these cases, the failure to follow the rule of law has given rise to controversy and public disquiet about the future of the law in Hong Kong. This reaction itself suggests that the rule of law is regarded as a public good in Hong Kong. However, these cases also raise the fear that mainlandisation will dilute the rule of law in Hong Kong.

A real post-1997 fear is that the judicial autonomy of Hong Kong is being threatened by the repeated interventions of the Standing Committee of the National People's Congress (NPCSC) in Beijing. The Hong Kong judiciary, which is supposed to be independent from the mainland, consists of the Department of Justice, the courts and other agencies. Headed by the Secretary for Justice, the Department of Justice prosecutes crimes and provides advice to agencies such as the police. The highest court in Hong Kong is the Court of Final Appeal, which hears appeals on civil and criminal matters from the High Court. The High Court (comprising the Court of Appeals and the Court of First Instance), hears appeals on all civil and criminal matters from the Court of First Instance and the District Court. It also hears appeals from the Lands Tribunal and various other tribunals and statutory bodies. The Court of First Instance hears both civil and criminal matters with unlimited jurisdiction. It also hears appeals from the Magistrates' Courts, the Small Claims Tribunal, the Obscene Articles Tribunal, the Labour Tribunal and the Minor Employment Claims Adjudication Board. For criminal trials, judges of the Court of First Instance sit with a jury of seven or nine, according to the judge's direction. The District Court hears civil

[47] Lo, T. Wing Ibid.

cases where the matter in dispute is valued between HK$50,000 but cap at HK$1 million and criminal cases limited to 7 years' imprisonment.[48]

Although the Court of Final Appeal is Hong Kong's highest court, under Article 158 of the Basic Law, the power of final interpretation of the Basic Law (Hong Kong's 'mini constitution') is vested in the Standing Committee of the National People's Congress (NPCSC). This power is derived from the Constitution of the People's Republic of China. However, reflecting the spirit of 'One Country Two Systems', Article 158 of the Basic Law also authorises the Hong Kong courts to interpret the law on their own, except for provisions that concern affairs that are a) the responsibility of the Beijing central government, or b) concern the relationship between the central government and Hong Kong.

Since 1997, there have been a number of occasions when the NPCSC has interpreted the Basic Law. This has prompted Lo to ask, "*who is the boss? Hong Kong's Court of Final Appeal or Beijing's NPC?*"[49] For example, in 1999, a case came before the Court of Final Appeal relating to the right of abode of mainland children born to Hong Kong parents. The Court of Final Appeal added that:

> "*Hong Kong courts can interfere with acts of the NPC if they breach the Basic Law. Interpretation of the Basic Law is to be carried out by the Court of Final Appeal, not the NPC, if the main issue in the case is within Hong Kong's autonomy…Courts should be reluctant to allow restrictions to be imposed on human rights enshrined in the Basic Law.*"[50]

---

[48] See Judiciary of Hong Kong, [Online] [cited:11/3/2012], at: <http://www.judiciary.gov.hk/en/crt_services/pphlt/html/guide.htm>.
[49] Lo, T. Wing, (2012) Op Cit.: p. 633.
[50] Lo, T. Wing, (2012) Op Cit. :p. 633, see also BBC News (22 May 2000) 'Case tests Hong Kong Autonomy' website:< http://news.bbc.co.uk/2/hi/asia-pacific/759385.stm> , [Visited 1/5/2013].

The verdict of the Court of Final Appeal led to tensions with the central government in Beijing, which regarded the verdict as a direct challenge to the NPCSC's powers and its ultimate political status. In the PRC, the law is explicitly an instrument of Communist Party policy. Beijing subsequently instructed the Hong Kong government to correct the Court of Final Appeal ruling. The Hong Kong government then passed a law that allowed the Chief Executive to request that the NPCSC interpret the ruling on Basic Law Article 24 concerning the right of abode of mainland born children. Ultimately, the Court of Final Appeal was forced to 'revisit' its decision, a move widely regarded as undermining Hong Kong's legal autonomy.[51]

The NPCSC has made further interpretations of the Basic Law that have again prompted protests among members of the legal profession who assert that the Court of Final Appeal should have the right to interpret the Basic Law.[52] As a result, Hong Kong's legal professions have become the 'defenders' of the rule of law. As Lo states, the legal profession has *"tried to minimize Hong Kong's legal convergence with mainland China*".[53]

Another major clash between Beijing and Hong Kong over the rule of law occurred when the HKSAR government was instructed by Beijing to introduce Article 23 into the Basic Law to regulate against subversion. Article 23 is a sensitive and politically controversial piece of legislation. Although many

[51] On June 30, 1999, 600 legal professionals launched a demonstration against the government's request for an interpretation of the Basic Law. The group stood silently outside the Court of Final Appeal to symbolise the death of the independence of Hong Kong's justice system.
[52] See Lo, T. Wing, (2012) Op Cit.: p. 634. See also Wai Keung Tam, (2013) Legal Mobilization Under Authoritarianism: The Case of Post-Colonial Hong Kong. Cambridge: Cambridge University Press.
[53] Lo, T. Wing, (2012) Op Cit.: p. 634.

countries have enacted this kind of national security law, the spirit of Article 23 was new to post-colonial Hong Kong.

Given the track record of the CCP and the Chinese government,[54] the very idea of Article 23 was enough to send chills down the spines of many in Hong Kong. As a result of the Article, many Hong Kong citizens became *"concerned with how national security would be interpreted and applied in the city*".[55] The move to enact Article 23 triggered mass protests and public outcry, with half a million people taking to the streets to march against the legislation in 2003. Eventually, the Hong Kong government put the National Security Bill on hold indefinitely. As a result, the rule of law[56] in Hong Kong has been temporarily shielded from being 'mainlandised'.

The prospect of legal practices from mainland China seeping into Hong Kong's legal system worries many people in Hong Kong, as does the possibility of mainland-style illegal practices. The Assistant Commissioner of the Hong Kong Customs and Excise Department, Albert Ho, argued that:

> "*Post 1997, cross-border crimes between Hong Kong and Mainland China are on the increase due to close by with China. Especially money laundering is increased between Hong Kong and mainland China, as Mainland China's economy is booming. [There are] differences in legal concept, and a high volume of people and goods exchanged between the two places. These crimes are more often than not highly and well organized by syndicates connected to Hong Kong and the Mainland… These kind of [criminal] activities are harming Hong Kong's reputation, particularly harming Hong Kong's*

[54] See Lee, F.L.F. Chan, J.M. (2011) Media, Social Mobilization and Mass Protests in Post-Colonial Hong Kong: The Power of a Critical Event. London: Routledge, p. 39.
[55] Lo, T. Wing, (2012) Op Cit.: p. 634.
[56] See Lo ibid.

> *global standing as an international financial centre. This is why the Hong Kong authorities [including the police, customs and excise] must protect Hong Kong's reputation, by enforcing the law rigidly*."[57]

As an example, Ho cited a case in which goods were sent to mainland China and money came back to Hong Kong, via both traditional means and through an Internet Banking account.[58] It is feared that such cases of money laundering will damage Hong Kong's reputation as a commercial centre, which has taken decades to build. Organised crime such as corruption and economic crimes such as Internet banking fraud and money laundering, are on the rise, partially due to this 'China factor'. According to a China Daily report in 2012:

> "*Major cross-border crimes in recent years include Mainland Chinese in Hong Kong, criminal enterprises involving fraud, theft, deception and forgery. In 2011, 377 mainland residents were arrested for committing a crime in Hong Kong. From 2007 to 2011, the number of mainland residents caught for serious offences varies, but definitely increased from 96 in 2007 and 308 in 2011 [a twofold increase in 4 years]*."[59]

These types of crimes are likely to affect Hong Kong's reputation as a 'clean' city in which to do business. In this thesis, I examine whether the Hong Kong government maintains a watchful eye on cross-border economic crimes or whether, as some argue, since 1997, the government has relaxed its control over the wheeling and dealing of the tycoons on whom it relies for political support. In particular, I examine how the government and its 'policing' agencies react when economic crimes, such as internet banking fraud, threaten Hong Kong's

---

[57] Ibid.
[58] Albert Ho, Assistant Commissioner of Custom and Excise Department, Hong Kong SAR Government, speaking at the invited, International Conference on Asian Organized Crime, 2nd May 2013, City University of Hong Kong.
[59] Deng, A. (June 21 2012) 'Two laws one common cause' China Daily Newspaper, website: < http://www.chinadailyapac.com/article/two-laws-one-common-cause>. [Visited 5/5/2013].

international reputation. In this regard, I inquire whether the interests of the government are still the same as those of the commercial elites?

The Political Environment

One of the arguments of this thesis is that political environments (i.e. traditions, structures and organisations) shape the ways in which different countries 'police' crimes such as Internet banking fraud. The Hong Kong government, which is executive led and highly centralised, governs a semi-authoritarian state rather than a democracy. This political structure is a legacy of British colonialism. Hong Kong was first ceded to the British Empire from China in 1841 and was regarded from the outset as a centre for trade and commerce. For instance, the Hong Kong and Shanghai Banking Corporation (HKSBC, now HSBC) was established in 1865, "*to finance intra-regional trade among the open ports of China, Japan and the Philippines for which it would engage in financing trading facilities*".[60]

In the 1980s, Hong Kong experienced two fundamental shifts: the signing of the Sino-British Joint Declaration in 1984[61] and the wholesale shift of manufacturing from Hong Kong to the mainland after China introduced its open door policy in 1978.

60 Tsang, S. (2004) A Modern History of Hong Kong, HK: Hong Kong University Press, p. 58. The HKSBC serviced the local steamship line, docks, tug boats and small industrial enterprises. The HKSBC soon established a role as an exchange bank, linked with Westminster Bank in London. This enabled it to tap into the London financial market. The bank subsequently flourished as a bridge between the financial world dominated by silver in China and sterling in London.

61 Tang, J.T.H., Ching, F. (1994) 'The MacLehose-Youde Years: Balancing the Three-Legged Stool' 1971-86', in Chan, M.K. (ed.) Precarious Balance: Hong Kong between China and Britain, 1842-1992. Hong Kong: Hong Kong University Press, p. 160.

**Table 1.6: The Percentage of Business Elites Appointed to the Legislative Council (1964-1971)**

| | 1964 | 1965 | 1966-67 | 1968-69 | 1970-71 |
|---|---|---|---|---|---|
| **Established Rich** | 66.0% | 41% | 46% | 38.5% | 30.8% |
| **New Rich** | 18.5% | 25% | 23% | 38.5% | 53.7% |

*(Source: King, A.Y.C. (1981) 'Administrative Absorption of Politics in Hong Kong: Emphasis on the Grass Roots Level', in King, A.Y.C. Lee, R.P.L. (Eds.), Social Life and Development in Hong Kong, HK: The Chinese University Press, p. 136)*

As Table 1.6 shows, by the end of the 1970s, the wealth in Hong Kong had mostly shifted to the Chinese 'nouveaux riche'. The 'nouveaux riche' tended to acquire their wealth through industrial and manufacturing activities, and later through property development. Subsequently, political power also shifted towards the 'nouveaux riche',[62] and their economic and business interests dominated governmental policies. As Goodstadt notes, "*such alliances survive even today after the British rulers have gone. Chinese leading merchants [have] become the Chinese political elite*".[63]

The pre-eminence of the business elite is important because Hong Kong has never been a democratic society.[64] According to Loader and Walker, the key role of the police in such authoritarian states is to protect the interests and ideology of

[62] Prior to the direct election of the Legislative Council in 1991, in order for the government to collect views and opinions from Hong Kong Society, the Hong Kong government (usually the Governor) appointed social elites (mostly businessmen or wealthy individuals) to act as unofficial members of the Legislative Council, to advise the Governor from time to time, to make and enact Laws and to serve on the Executive Council (even today, there are 14 unofficial member serving on the Executive Council, most of whom are wealthy businessmen). The official members, or ministers, are the principal officials of the Hong Kong Government. Within just seven years, unofficial Legislative Council members from the 'nouveaux riche' increased from 18.5 per cent in 1964 to 53.7 per cent in 1971, while those from the established rich decreased from 66 per cent in 1964 to 30.8 per cent in 1971.

[63] Goodstadt, L.F. (2005) Uneasy Partners: The Conflict between Public Interest and Private Profit in Hong Kong. Hong Kong: Hong Kong University Press, p. 117.

[64] However, in July 2009, the Hong Kong government proposed a green paper implementing universal suffrage for the Chief Executive in 2017, to be followed by elections for the Legislative Council (LegCo). See the Hong Kong Government, (2009) 'Green Paper on Constitutional Development'. Hong Kong: Hong Kong Government, para.5.15 (ii) & (iii)-5.16, pp. 44-45.

the regime and the private interests that it supports.[65] In Hong Kong, these interests are trade and commerce. However, in the run-up to 1997 some commercial elites deserted the British administration to curry favour with the leaders on the mainland, in the hope of pursuing trade in mainland China. Therefore, it is no longer clear whether the aims of the current post-1997 administration and the commercial elites in Hong Kong are unified, as some may wish to make a profit at any cost, even if it means undermining the rule of law and even-handed policing.

The Economic Environment

I also argue that the economic environment (i.e. structures, organisations, traditions, resources) is another key factor influencing the manner in which a society is policed. Traditionally, the Hong Kong administration has adopted a 'laissez faire' ethos of maintaining conditions conducive to trade.[66] Ghose[67] suggested that when Hong Kong's banking and financial institutions were first established in the 1840s, the colonial authorities were mainly concerned with maintaining security and creating a business environment conducive to free trade. In keeping with this, there was minimal government control and regulation of the private sector (such as the banking and financial sectors). This laissez-faire economic approach has continued to this day.

[65] Loader, I., Walker, N. (2007) Civilizing Security. Cambridge: Cambridge University Press, p. 77.
[66] This 'laissez faire' ideology is still very much alive in the governance of Hong Kong in the 21st Century.
[67] Ghose, T.K.. (1987) The Banking System of Hong Kong, Singapore: Butterworks, p. 17.

The story of the Hong Kong 'miracle' is well-established. In the 1950s, Hong Kong's economy took off. The fall of Shanghai to the communist forces in 1949 proved pivotal for Hong Kong's subsequent industrialisation. Industrialists from Shanghai moved into Hong Kong, bringing their financial and intellectual capital.[68] It has been estimated that two-thirds of the initial investment in Hong Kong came from Shanghai industrialists.[69] In 1951, the Korean War led the United Nations to impose an embargo on trade with mainland China, thus immediately ending Hong Kong's role as an entrepot trading centre. Hong Kong was thereby compelled to explore new sources of income. Riedel argues that the only available avenue was industrialisation.[70] Two vital factors made this new path a possibility: the infusion of Shanghainese financial capital and their industrial business experience which gave the colony a ten-to fifteen year start over the rest of East Asia,[71] and refugees from China, who provided an instant pool of cheap labour. By the 1960s, Hong Kong's economy had begun to over-take that of its colonial forebear in terms of economic growth, success and prosperity.

With the aid of Chinese entrepreneurship, a flexible labour force, openness to technological innovation and a global economy, Hong Kong was able to flourish. The government policy of "positive non-interventionism" was also a key factor in Hong Kong's growth. This phrase was coined by Sir Philip Haddon-Cave, a

[68] See Wong S.L. (1988) Emigrant Entrepreneurs: Shanghai Industrialists in Hong Kong. Hong Kong: Oxford University Press.
[69] See Riedel, J. (1974) The Industrialisation of Hong Kong. Tubingen: J.C.B. Mohr.
[70] See Riedel, J. (1974) Ibid.
[71] Carroll, J.M. (2005) Edge of Empires: Chinese Elites and British Colonials in Hong Kong, Cambridge: Harvard University Press, p. 57.

former Financial Secretary, to describe Hong Kong's distinct version of laissez-faire capitalism:

> "*The government recognises the need to impose ground rules and legal constraints to mark out the area within which market forces are allowed to operate. So there is a large body of legislation governing the formation and activities of companies and the performance of contracts, and the government regulates the banking industry and other financial institutions such as the stock exchanges and commodity trading…*"[72]

However, several economic and bank failures between the 1960s and 1980s resulted in the markets becoming increasingly regulated, to such an extent that by the 1980s the Securities and Futures Commission (FSC) was accused of enforcing too strict a superintendence of commercial activities.[73] Nonetheless, the government was keen to ensure the strict regulation and 'policing' of banks to maintain Hong Kong's reputation as a major international financial centre. By the 1980s, the Hong Kong Police had also started to equip themselves to help manage the needs of the Hong Kong economy.[74] By the 2000s, Hong Kong had

[72] Miners, N. (1998) Fifth Edition. The Government and Politics of Hong Kong. Hong Kong: Oxford University Press, pp. 47-9.
[73] Ibid.
[74] By the 1990s, Hong Kong had become a cosmopolitan city, one of the most prosperous in Asia. There was full employment and relatively high levels of income; 28% of Hong Kong households owned their homes.[74] As Wong et al. observe, the Gross National Product (GNP) per capita amounted to US$6,230 (approximately HK$48,594) in 1986, the third highest in Asia after Japan and Singapore. As Table 1A shows, the Gross Domestic Product (GDP) grew more than 4 times within 18 years. By 1984, Hong Kong's GDP had reached HK$178,071 million up from HK$43,417 million in 1966.

**Table 1A: Hong Kong Gross Domestic Product (1966-1984):**

| | **1966** | **1971** | **1976** | **1981** | **1984** |
|---|---|---|---|---|---|
| **Gross Domestic Product (HK$ million)** | 43,417 | 59,921 | 89,887 | 150,139 | 178,071 |
| **Per capita GDP (HK$)** | 11,961 | 14,812 | 20,228 | 29,130 | 33,197 |
| **Electricity Consumption (Million Megajoules)** | - | 17,609 | 26,190 | 40,427 | - |
| **Telephone Lines Working** | - | 565,453 | 909,679 | 1,278,866 | - |

established itself as an international global financial and banking centre, secured by the rule of law.

On 1 July 1997, the Chinese government appointed Tung Chee-hwa as the first Chief Executive of the Hong Kong Special Administrative Region (SAR). Tung was regarded with some suspicion locally because although he was a local shipping tycoon, his company was financially beholden to the People's Republic of China.[75] He was thus seen as pro-big business and pro-Beijing. As Lau states, Tung's style was paternalistic and his decision making was characterised by top-down policy making and limited public consultation.[76] According to Lau:

> *"The business elites believed that the new administration, headed by a prominent member from their rank, as compared with the already pro-business colonial regime, would be even more willing to serve the interests of the business community. They expected to forge a closer bond between money and politics."*[77]

Because Tung was more pro-business, it was feared that he would give businesses free-rein to conduct their dealings, relax the policing of the financial sector and allowing dubious cross-border business dealings. One issue for this thesis if whether there is any evidence, in the data, that this was been the case or whether the regulatory authorities in Hong Kong strived to rein in the more dubious dealings of cross-border commercial actors.

---

*(Source: Cited in Table 15, Chan K.L. (1989) 'Demographic Setting of Hong Kong: Developments and Implications', in Kwan, A.Y.H. (Ed.) Hong Kong Society, Hong Kong: Writers & Publishers, p. 35*)

[75] Tsang, S. (2004) Op Cit.: p. 266.

[76] Lau, S.K. (2002) 'Tung Chee-hwa's Governing Strategy: The Shortfall in Politics', in Lau, S.K., (ed.) The First Tung Chee-hwa Administration. Hong Kong: The Chinese University Press, p. 16.

[77] Lau, S.K. (2002) Op Cit.: p. 9.

Banking

Banking is central to the Hong Kong economy and its financial success. Therefore, it is worth investigating how the government and its agencies in Hong Kong react to Internet banking fraud, which is likely to have a negative effect on the economy?

According to the World Economic Forum Financial Development Index,[78] in 2011, Hong Kong overtook the US and the United Kingdom (UK) to become ranked first in the world for financial development. The World Economic Forum indicated that this success was due to Hong Kong's institutional and business environment, financial stability, banking financial services, non-banking financial services, financial markets and financial access. Today, Hong Kong is well recognised as a leading international financial and banking centre. Banking policies play a key role in maintaining Hong Kong's competitiveness and the government is well aware of the importance of the financial sector to the Hong Kong economy. This also means that the government keeps a watchful eye on economic crimes, including Internet banking crime.

In the early 1980s, the Hong Kong economy was also affected by China's open door policy. Hong Kong soon became an entrepot for Chinese trade. Overseas multinational firms were attracted by the opportunities offered by the opening up of mainland China, and began to set-up their regional offices in Hong Kong, including representative offices for management, technology, and for research

[78] See World Economic Forum, The Financial Development Report 2011, [Online] [cited 01/01/2012], at: < http://www.weforum.org/reports>.

and design backup for factories in mainland China.[79] This helped boost the growth of the service industries, making Hong Kong an international and regional hub for professional services, such as accounting, insurance, shipping, banking and back office support. As Henderson states, "*Hong Kong's economy has survived and prospered because of the service functions it performs for China's economy, [such as] trading connections, managerial expertise, finance, professional skills*".[80] Hong Kong thus acquired a pool of well qualified, highly educated local technology graduates,[81] as well as accountants and bankers. By the 2000's, Hong Kong was providing financial and business services to Chinese companies trading with the West. As Sassen explains:

> "*The specialisation of Hong Kong in financial and business services increased as manufacturing jobs moved to the mainland [China]. And Chinese companies used the Hong Kong Stock Market when they wanted to raise money.*"[82]

According to a City of London Report, the Hong Kong stock market also increased significantly between 1992 and 2005. The biggest increase was in the capitalisation of the equity market, which had reached US$26,544 billion by the end of 2007.[83] Table 1.7 shows the ranking of global financial centres as of March 2009, where Hong Kong continues to be ranked 4th in the world.

---

[79] Chen, K.Y.E., Nyaw, M.K. and Wong, T.C. (Eds.) (1991) Industrial and Trade Development in Hong Kong. Hong Kong: University of Hong Kong, p. 35.
[80] Henderson, J. (1999) 'Uneven crises: institutional foundations of East Asian economic turmoil'. Economy and Society. Vol.28 Number 3, p. 344.
[81] See fuller details in Henderson, J. (1989) The Globalisation of High Technology Production: Society, Space, and Semiconductor in Making of the Modern World. London: Routledge.
[82] Schifferes, S. (Wednesday, 27 June 2007) 'Hong Kong v Shanghai: Global Rivals'. BBC News. [online] [cited-:14/03/2009], available from:< http://news.bbc.co.uk/1/hi/business/6240994.stm>.
[83] The City of London. (October 2008) 'The Future of Asian Financial Centres- challenges and opportunities for the City of London. London: Research Republic, para. 3.4.2, p. 40.

**Table 1.7: The Top Ten Global Financial Centres**

| Financial Centre | 2008 (September) Ranked | 2009 (March) Ranked |
|---|---|---|
| London | 1 | 1 |
| New York | 2 | 2 |
| Singapore | 3 | 3 |
| Hong Kong | 4 | 4 |
| Zurich | 5 | 5 |
| Geneva | 6 | 6 |
| Tokyo | 7 | 15 |
| Chicago | 8 | 7 |
| Frankfurt | 9 | 8 |

*(Source: The City of London. The Global Financial Centre Index, March 2009, p.4)*

Moreover, as Table 1.8 shows, a considerable number of fully licenced international banks are authorised to operate in Hong Kong by the Hong Kong Monetary Authority. In 2003, 134 fully licenced overseas banks were authorised to operate in Hong Kong. This increased to 142 in 2007.

**Table 1.8: Total Number of Licenced Banks Operating in Hong Kong**

| Regions | 2003 | 2004 | 2005 | 2006 | 2007 |
|---|---|---|---|---|---|
| Asia and Pacific (in bracket Hong Kong local banks) | 73 (13) | 74 (12) | 75 (12) | 79 (11) | 82 (11) |
| Europe | 42 | 41 | 40 | 41 | 41 |
| Middle East | 2 | 1 | 2 | 1 | 1 |
| North America | 16 | 16 | 15 | 16 | 17 |
| South Africa | 1 | 1 | 1 | 1 | 1 |
| **Total** | **134** | **133** | **133** | **138** | **142** |

*(Source: Hong Kong Monetary Authority. (2007) Annual Report 2007, Table D, p.207)*

Along with tourism and trading and logistics, financial and professional services have become the key industries in Hong Kong. The 2010 Census and Statistics Department report[84] shows that these four key industries accounted for 55.6% of

[84] See Census and Statistics Department, [Online], at: <http://www.censtatd.gov.hk/hong_kong_statistics/statistical_tables/index.jsp?subjectID=12&tableID=190>.

Hong Kong's GDP in 2009, of which financial services accounted for 15.1% and professional services 13.1%. Together, the two industries accounted for 28.2% of the Hong Kong's GDP, which confirms that financial and professional services make a significant contribution to the economy. I argue that this is one reason why the Hong Kong government rigorously controls and polices the financial and banking sectors, prosecuting and punishing those who harm it.

Policing and the Criminal Justice System

Because Hong Kong's 'clean' image is key to its international reputation as a financial centre, the government is likely to consider the policing of economic crimes such as Internet banking fraud to play an important role in protecting this image. However, does this mean that the police, courts and other regulatory agencies take a hard line on such crimes?

In theory, the Hong Kong police force is an arm of the government and can respond quickly to changing government priorities. Moreover, because the government itself is not democratic, but executive led. In theory, therefore, the government is able to exercise tight control over the police and other allied agencies. Does this mean that, if the government decides that economic crimes like Internet banking fraud are a priority then evidence should suggest that the criminal justice system takes a hard line in policing such crimes?

The Hong Kong criminal justice system is headed by the Secretary for Security and the activities of the various departments are supervised and co-ordinated by the Chief Secretary for Administration, who is in fact deputy to the Chief

Executive of Hong Kong and the official head of the civil service. The organisational structure of each branch or department within the criminal justice system is tightly controlled from the centre and decision making is top-down.

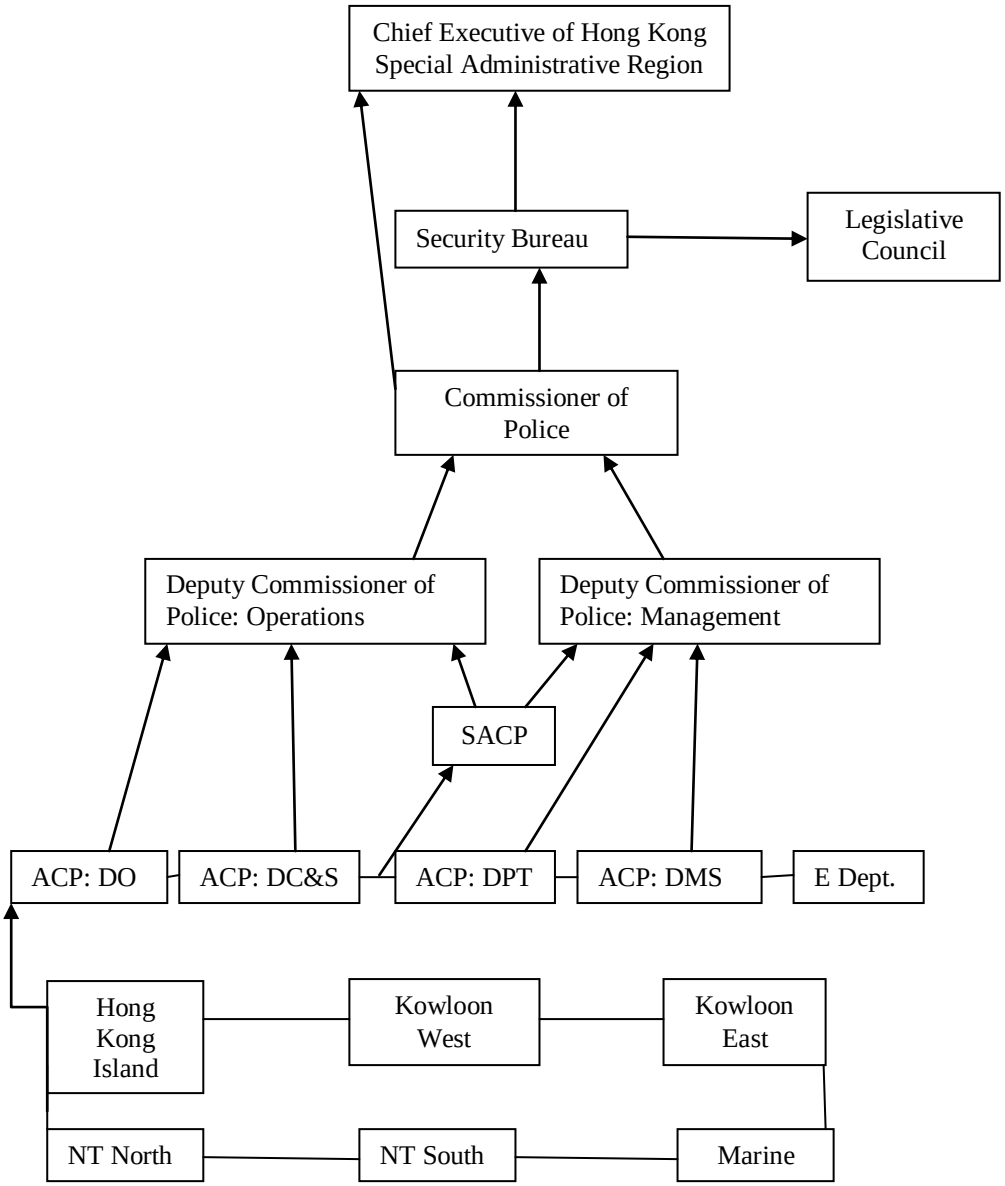
The Hong Kong Police Force is directly answerable to the Secretary for Security and is classified as a 'disciplined service'.[85] Together with the Securities and Futures Commission and other disciplinary services (such as the Independent Commission Against Corruption (ICAC)), the police form the 'front line' agencies of the criminal justice system. The ICAC 'polices' all fraud involving corruption, including that conducted both online and offline. However, unlike the police, the ICAC is not under the ambit of the Secretary for Security and is by design independent from the rest of the civil service. The ICAC is answerable solely to the Chief Executive of Hong Kong.

The Hong Kong Police and the ICAC are the two main agencies that handle economic crime, although other agencies also take part in investigations (including non-government bodies such as banks, insurance companies, credit card companies, and so on). A specialist unit within the Hong Kong Police (the Technology Crime Division) is tasked with policing technology-related crimes, although other specialised units such as the Commercial Crime Bureau also play a large role in investigating such matters. There is a great deal of coordination

[85] See Op Cit. p. 56. In addition to the police, other government departments classified as disciplined services include the Fire Services Department, the Correctional Services Department, the Immigration Department (a specialist unit for dealing with illegal immigrants that carries fire arms), the Customs and Excise Department (almost all of the staff are trained to use fire arms, some border control officers are armed when on duty and all drug squad officers are always armed when on duty) and the Government Flying Services.

and cooperation between these departments. The organisational structure of the Hong Kong police is shown in Diagram 1.1.

**Diagram 1.1: The Organisational Structure of Hong Kong Police**




*Source: The Hong Kong Police*

SACP: Senior Assistant Commissioner of Police
ACP: Assistant Commissioner of Police
DO: Director of Operation A Dept.; DC&S: Director of Crime & Security B Dept.; DPT: Director of Personnel & Training C Dept.; DMS: Director of Management Services; E Dept.: Civilian Officer as Director of Finance Administration & Planning.
NT: New Territory

As an arm of government, the Hong Kong police must obey the orders of the Chief Executive of Hong Kong. The Hong Kong Police Force Ordinance (Cap 232 section 4) specifies that the Commissioner of Police is "subject to the orders and control of the Chief Executive".[86] The Commissioner of Police is appointed by and directly answerable to the Chief Executive. The police force as a whole is directly accountable to the government officials at the Security Bureau. The Secretary for Security, the Commissioner of Police and the Chief Executive can be called before the Legislative Council to explain their decisions on issues relating to policing. The Chief Executive may seek advice on policing at Executive Council meetings. The police also liaise with the District Fight Crime Committees established in each of the 18 districts in Hong Kong on matters concerning crime in the local area. The Committees play an advisory role to the government on measures to reduce crime and the members are almost all government appointed. As Hong Kong is not a democratic society, the priorities for policing in Hong Kong are not set by election manifesto, although they are now often decided in conjunction with the District Fight Crime Committees, the Legislative Council and various other local committees.

Ultimately, the policing priorities in Hong Kong are determined by the Commissioner of Police. The policing of Internet crime is one of the Commissioner's "operational priorities".[87] Moreover, two out of the seven

[86] Hong Kong Police Force Ordnance Cap 232, section 4. See also Traver, H. (2009) 'Hong Kong Police Force' in Gaylord, M.S. Gittings, D. Traver, H. (eds.) (2009)) Introduction to Crime, Law and Justice in Hong Kong. Hong Kong: Hong Kong University Press, p. 57.
[87] The Hong Kong Police, website: < http://www.police.gov.hk/info/cop/2013/p3_e.html>. [Visited 16/7/2013].

Commissioner of Police's operational priorities[88] are related to economic crimes (such as quick cash crime, Internet crimes, and triads, syndicated, and organised crime).

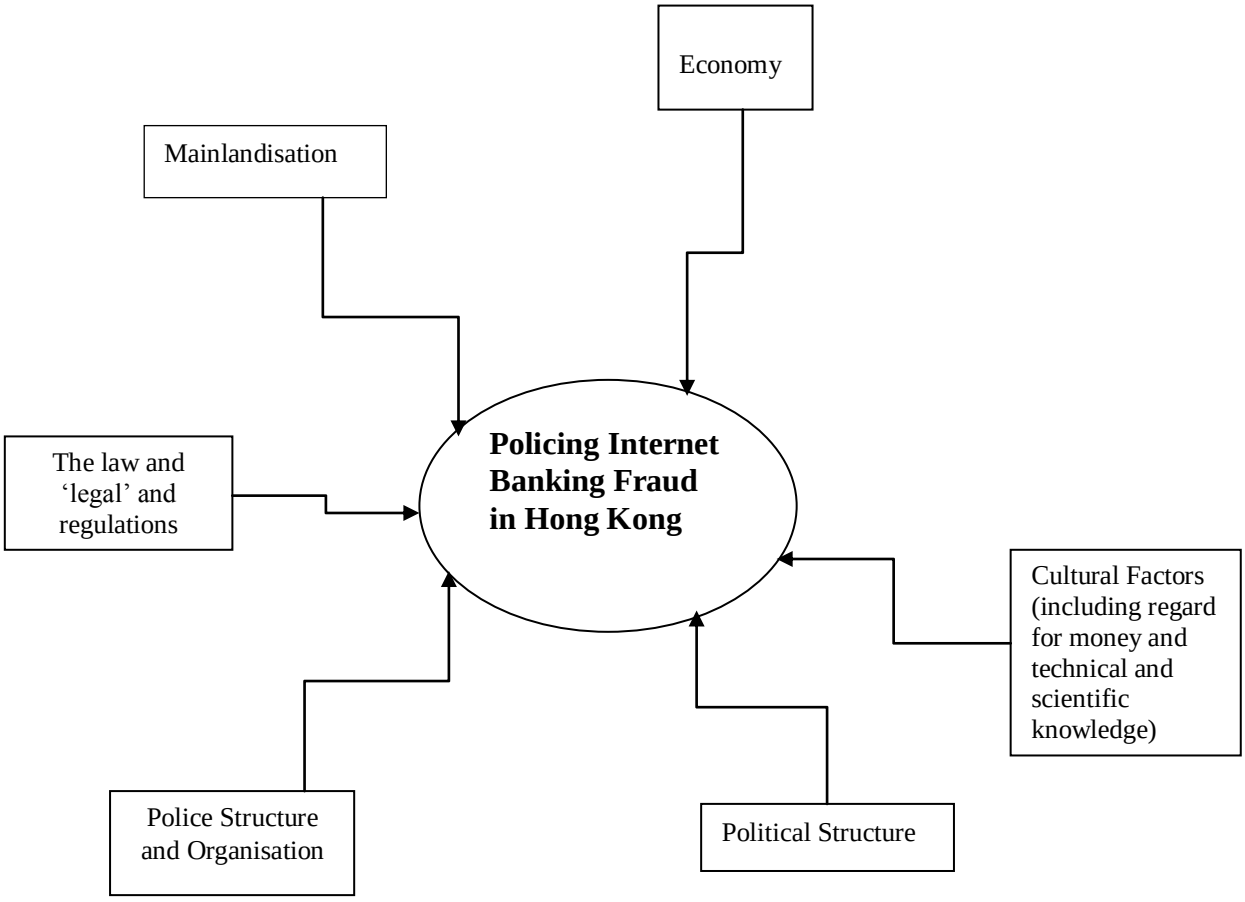
I argue that the operational priorities of the Hong Kong police reflect the influence of the dominant political and economic elites. For instance, the kinds of people who are appointed to and dominate at the Executive Council are largely dominated by prominent merchants and professionals. Accordingly, the priorities of policing are more likely to reflect the interests of the government officials at the highest level of government than those of the general public. Therefore, the interests and priorities of the government are likely to favour policies that protect the economy. In addition, the government in mainland China also sees Hong Kong primarily as an economic city. As Wong and Luk observe, "*It is often argued by both the HKSAR government and the Chinese central government that Hong Kong should be an economic city, not a political city, focusing mainly on economic development in lieu of political development."*[89] Because all government policies are fundamentally geared towards protecting the economy, any illegal activities that harm the economy, including Internet banking fraud, are likely to be treated as serious crimes that deserve the full force of the law.

[88] The Hong Kong Police, website: < http://www.police.gov.hk/info/cop/2013/p2_e.html>. [Visited 16/7/2013].
[89] Wong, W. Luk, S. (2007) Economic Policy, in Lam, W. M. Lui, P.L.T. Wong, W. Holliday, I. (ed.) Contemporary Hong Kong Politics: Governance in the post-1997 Era. HK: Hong Kong University Press, p. 200.

Summary

In this thesis, I explore further whether and how factors such as the economic, political and cultural environment, 'mainlandisation' and the structure of the police force outlined here (see Diagram 1.2) affect the occurrence and policing of Internet-based economic crimes in Hong Kong, such as Internet banking fraud. The questions I examine include how does culture influence people's use of Internet banking? Does the level of technological and financial development affect the way such crimes are committed and policed? Does Hong Kong's semi-authoritarian, non-democratic and executive-led state structure affect the priorities of the police and the courts? How has the process of mainlandisation affected the independence of the courts? What kinds of cross-border Internet economic crimes are being committed between Hong Kong and the mainland? Has greater integration with the mainland economy affected the types of Internet crimes that are committed in Hong Kong? Has Hong Kong adopted a 'laissez-faire' approach to policing this type of crime or do the authorities (the police, the ICAC, HKMA, SFC and the government) actively regulate the Internet to protect Hong Kong's standing as an international financial centre? These are the kinds of questions I examine in the following chapters.

**Diagram 1.2: Factors Influencing the 'Policing' of Internet-related Economic Crimes 'Internet Banking Fraud'**



# Chapter Two
# Literature and Methodology

## Introduction

According to Reiner and Newburn, "*Policing maybe carried out by a variety of social institution, agents or mechanisms, not just the police*".[90] One of the main aims of this thesis is to examine how factors such as the law, culture, economy, politics and history shape the 'policing' of Internet banking fraud by banks, the police, prosecution and courts in Hong Kong. To achieve this, I examine how these parties identify, investigate, prosecute and sentence such Internet economic crimes. As indicated in Chapter One, I adopt a socio-legal theoretical framework in this thesis. Socio-legal research examines how the law, the legal system, lawyers, judges and courts relate to the wider social, economic and political environment. In Chapter One, I outlined the main factors that contribute to the socio-legal environment in Hong Kong.

In this chapter, I present the methodological framework for the empirical investigation of the decision-making processes of the banks, police, prosecution and courts. Because I want to know how these institutions identify, investigate and prosecute Internet banking fraud, I have chosen methods that are appropriate for interviewing small numbers of key decision-makers in the banks, the police and the Department of Justice. I also analyse a sample of Appeal Court cases that deal with Internet banking crimes. The interview data are used to inform my understanding of how and why the police, prosecution and courts handle these cases. The case sample covers Appeal Court cases between 1999 and 2012. It

[90] See Reiner, R. and Newburn, T. (2008) 'Police Research', in King, R. and Wincup, E. (eds.) Doing Research on Crime and Justice, Oxford: Oxford University Press, p. 343.

provides evidence of the kinds of cases brought to trial in Hong Kong, whether they ended in conviction and, if so, what kind of punishment the defendants received. I also conduct a survey of the literature on the criminal justice and political systems in Hong Kong and on Hong Kong's social development, laws, culture and integration with mainland China. I also examine secondary data, such as newspapers, government reports, private sector reports, and government statistics on the economy, trade and technological development.

Literature on Economic Crime

The general literature on economic crime covers a wide range of topics, ranging from criminological work on white-collar crime in general, to work on particular types of crime, such as various kinds of fraud, money laundering and cyber-related economic crime.

The existing criminology research focuses on both high-level economic crime and more low-level workplace crime. Edwin Sutherland's seminal article, 'White-Collar Criminality',[91] challenged the traditional criminological view that the lower classes commit the most crime. Sutherland contended that respectable businessmen and professionals also committed crime in their occupations, which he labelled 'white-collar crime'. However, in light of the emergence of the Internet and smart-phone technologies over the past twenty years, Sutherland's argument needs amendment. Today, it is possible for people in less privileged populations to commit what were once strictly 'white-collar' crimes (such as

[91] Sutherland, E.H. (February, 1940) 'White-Collar Criminality', American Sociological Review, Vol. 5, No. 1.

fraud and embezzlement) while on a bus, in a private car, at home or in a cyber-café, rather than in the office.

However, economic crime is still regarded as elite, 'white collar' crime in much of the literature. For instance, Payne's 2012 book, *White-Collar Crime*,[92] still focuses on crime in the workplace, while the updated 2013 version[93] of the book discusses the various responses to the problem. On the other hand, David Simon's *Elite Deviance*,[94] also published in 2012, discusses the ways in which economic and political elites have benefited by exploiting the loopholes in the US regulatory system following of the de-regulation of the US banking system in the 1980s.

The weaknesses and strengths of the global regulatory system are also explored by Edelbacher et al. in their 2012 book, *Financial Crimes*.[95] This volume of essays examines whether a global effort could prevent the 2007 global financial crisis from happening again. This book also highlights the difficulty in policing the crime associated with trans-border financial transactions. In his 2004 book, *Global Financial Crime*[96], Masciandaro also places such crimes in an international context to give some insight into money laundering and the funding of global terrorism. While money laundering is a transnational crime, it is also a traditional economic crime that has moved from the real world to the virtual world with the advancement of Internet technology. In this regard, the nature of

[92] Payne, B.K. (2012) White-Collar Crime. Thousand Oaks: Sage.
[93] Payne, B.K. (2013) White-Collar Crime. Thousand Oaks : Sage
[94] Simon, D.R. (2012) Elite Deviance. New Jersey: Pearson.
[95] Edelbacher, M. Kratcoski and P. Theil, M. (2012) (Eds.) Financial Crimes: A Threat to Global Security, London: CRC Press.
[96] Masciandaro, D. (ed.) (2004) Global Financial Crime. Aldershot: Ashgate.

crime has not changed so much as the way in which it is now being committed. In their 2012 book, the *Internationalisation of Corruption*,[97] Fletcher and Herrmann also explore the problem of corruption in a global context. They argue that the nature of corruption has changed in the 21st century, and is no longer confined to specific places or countries, or to the developing world. Rather, corruption has become a complex global issue that reflects the fact that the world is now highly integrated economically. As a result, when corruption occurs in one place it can now resonate globally.

Literature on Economic Crime in Hong Kong

Few studies focus specifically on economic crime in Hong Kong, at the elite or any other level. Most of the existing research deals with corruption, money laundering and organised crime or triad related issues.

Some of the earliest sociological work on corruption in Hong Kong was carried out by Henry Lethbridge. His 1985 book, *Hard Graft in Hong Kong*,[98] discusses in detail on how social, economic and political factors provided the conditions for corruption to take root in Hong Kong from the 1840s onwards. Examining the establishment of the Independent Commission Against Corruption (ICAC) in early 1974, which was founded to root out corruption. Lethbridge argues that people in Hong Kong were no longer prepared to accept the status-quo on corruption, which was wide-spread in society as whole, especially in the police. The social, political and economic changes in the 1960s (including Hong Kong's

[97] Fetcher, C. and Herrmann, D. (2012) The Internationalisation of Corruption: Scale, Impact and Countermeasures. Farnham: Gower.
[98] Lethbridge, H.J. (1985) Hard Graft in Hong Kong: Scandal, Corruption, the ICAC. Hong Kong: Oxford University Press.

rapid industrialisation) had transformed Hong Kong society and peoples' attitudes towards the government. As a result, the colonial government began to take decisive action to root out corruption to create a 'level playing field', on which it was believed anyone who worked hard enough might succeed. De Speville's 1997 book, *Hong Kong Policy Initiative against Corruption*,[99] provides a detailed analysis of the institution of the government's anti-corruption programme, summarising what has worked and what has not worked in Hong Kong.

Lo Tit-Wing's research on corruption in Hong Kong and China, particularly his 1993 book *Corruption and Politics in Hong Kong and China*[100] provides a more sociologically and politically-informed analysis. He draws attention to the different ways in which corruption is censured in communist China and Hong Kong. In early 1970s, combating corruption became a government priority in Hong Kong because the question of corruption was closely tied to the legitimacy of the colonial government. Lo concludes that the traditional way of looking at corruption is insufficient, because it ignores the structural conflicts and political dynamics underlying the creation and punishment of corruption. In particular, he argues that society is composed of different levels of conflicting goals and interests. In his 2003 essay, *Minimizing Crime and Corruption in Hong Kong*,[101] he offers an overview of the top political-criminal connections in Hong Kong. Moreover, in a co-authored article in 2009, 'Restricting Loans of Money to Hong

[99] De Speville, B. (1997) Hong Kong Policy Initiative Against Corruption. Development Centre of the Organisation for the Economic Co-operation and Development. Hong Kong.
[100] Lo, T. Wing, (1993) Corruption and Politics in Hong Kong and China. Buckingham: Open University Press.
[101] Lo, T. Wing, (2003) 'Minimizing Crime and Corruption in Hong Kong', in Godson, R. (ed.) Menace to Society: Politicial-Criminal Collaboration Around the World. New Brunswick: Transaction Publishers.

Kong Civil Servants',[102] Lo and Ngan adopt a social censure perspective to examine why the colonial administration put in place draconian measures to prevent bribery in the 1970s, which were not repealed even in the 1990s. (I adopt Lo and Ngan's research methodology in my analysis of the sample of court cases.) Scott's 2011 publication, *Corruption Control in Hong Kong*,[103] also looks at corruption from a legal perspective by examining the rules, regulations and policies on corruption in Hong Kong. More specific studies of bribery and corruption in Hong Kong include Etheradge's 1995 study, *Managerial Bribery and Corruption in Hong Kong*,[104] which aims to provide a model of the processes of decision-making with respect to managerial bribery and corruption.

Manion also compares the state responses to corruption in Hong Kong and China in her 2004 book, *Corruption by Design.*[105] Here, Manion looks at how Hong Kong's anti-corruption reforms have successfully rooted out widespread corruption, in contrast to the less successful reforms in mainland China in the 1980s. Even though Hong Kong and China share some important commonalities, such as Chinese culture and an absence of democracy, Manion concludes that Hong Kong differs greatly in most other aspects, in particular being an open capitalist economy, with a belief in the rule of law. Although China censured corruption much earlier than Hong Kong, China's anti-corruption initiatives have always been coloured by political motives, such as purging political opponents.

---

[102] Lo, T. Wing and Ngan, P. (2009) Restricting Loans of Money to Hong Kong Civil Servants: Social Censure or Violation of Human Rights? Crime, Law and Social Change. Vol. 52, No. 4.
[103] Scott, I. (2011) Corruption Control in Hong Kong: Rules, Regulations and Policies. Hong Kong: Department of Public and Social Administration. City University of Hong Kong.
[104] Etheredge, J. (1995) Managerial Bribery and Corruption in Hong Kong: Towards an Explanatory Model. Hong Kong: Business Research Centre, Hong Kong Baptist University.
[105] Manion, M. (2004) Corruption by Design: Building Clean Government in Mainland China and Hong Kong. Cambridge: Harvard University Press.

Literature on Internet Crime

Over the last twenty years, a great deal of criminological research has focused on the subject of Internet crime. For instance, in Pattavina's 2005 book, *Information Technology and the Criminal Justice System*,[106] discusses how the advancement of information technology is related to many issues in the criminal justice system, especially policing. In their 2007 book, *Cybercrime*,[107] Balkin et al. discuss the crime associated with digital networks and how the Internet has altered policing. In particular, they examine how the police have shifted to a new form of co-operation between the public and private sectors, and the increasing use of digital surveillance for law enforcement in the US.

UK publications in this area include David Wall's works both in 2000 *Policing the Internet*[108] and his 2007 book *Cybercrime*, [109] both of which examine the approaches for policing cybercrime from a broad perspective. Ian Walden's 2007 book, *Computer Crimes and Digital Investigations*,[110] also focuses on the legal processing of computer crime. Mathew Williams' 2006 book, *Virtually Criminal*,[111] takes a similar approach to Wall in examining the regulation of cybercrime from a broad perspective. Majid Yar's 2006 book, *Cybercrime and*

[106] Pattavina, A. (2005) (ed.) Information Technology and the Criminal Justice System. Thousand Oaks:Sage.
[107] Balkin, J. Grimmelmann, J. Katz, E. Kozlovski, N. Wagman, S. Zarsky, T. (2007) (eds.) Cybercrime: Digital Cops in a Networked Environment. New York: New York University Press.
[108] Wall, D. (2000) 'Policing the Internet: Maintaining Order and Law on the Cyberbeat', in Akdeniz, Y., Walker, C. and Wall, D. (eds.) The Internet, Law and Society. Harlow: Longman.
[109] Wall, D.S. (2007) Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity.
[110] Walden, I. (2007) Computer Crimes and Digital Investigations. Oxford: Oxford University Press.
[111] Williams, M. (2006) Virtually Criminal: Crime, Deviance and Regulation Online. London: Routledge.

*Society,*[112] focuses on the sociological nature of cybercrime. Yaman Akdeniz and Wall's 2000 book, *The Internet, Law and Society*, [113] focuses on issues relating to Internet child pornography and cyber privacy.

In 2010, Yvonne Jewkes and Majid Yar's *Handbook of Internet Crime*[114] brings together a range of studies on cybercrime published over past 25 years that form the basis of contemporary cybercrime research. The wide range of scholarship addresses the globalised nature of the crime and the discussion 'takes stock' of the latest research in the field, covering a wide range of issues, such as the imaginaries of cybercrime, the use of the Internet as a tool to spread international terrorism, the rise of cyber protection and civil society, the use of the Internet as a social media tool to spread political ideas, the recent increase in cyber homicide and suicide via the Internet, the increased use of private police to police Internet crime, how the sex industry has employed different Internet media to sell its products online and the issue of online identity theft.

In 2007, Fletcher's paper, "Challenges for regulating financial fraud in cyberspace",[115] provides an overview of how financial fraud operates in cyberspace and the best ways to address the problem. Fletcher concludes that an important factor in combating financial fraud in cyberspace is maintaining a close liaison between the policing partners. This issue is discussed in this thesis.

[112] Yar, M. (2006) Cybercrime and Society. London: Sage.
[113] Akdeniz, Y. Walker, C. Wall, D. (eds.) (2000) The Internet, Law and Society. Harlow: Longman.
[114] Jewkes, Y. Jar, M. (2010) (eds.) Handbook of Internet Crime. Cullompton: Willan.
[115] Fletcher, N.(2007) 'Challenges for Regulating Financial Fraud in Cyberspace.' Journal of Financial Crime, Vol. 14 (2), pp. 190-207.

In their 2008 book, *Securing the Information Infrastructure*,[116] Kizza and Kizza discuss 'cyberspace' as a dynamic information infrastructure that requires governmental level protection. They argue that the financial and banking system is an important wealth-making infrastructure that is increasingly dependent on 'cyberspace' and thus requires high-level legal and political protection. This point is pertinent to the aims of this thesis.

Moore's 2011 book, *Cybercrime*,[117]provides an introductory overview of the fast changing field of technology related crime and the US criminal justice system's response to this new threat, although the subject matter is of limited use in the Hong Kong context. Similarly, Reveron's 2012 edited collection, *Cyberspace and National Security*,[118] aims to fill the gap in our understanding of how cyberspace relates to US national security and explores the various government led approaches to advancing and defending 'American' interests in cyberspace.

In 2012, Awan and Bleakemore's *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*[119] explores cyber hate crime, cyber threats and cyber terrorism, and considers how cyber-terrorists can use the Internet to attack infrastructure, including financial infrastructure. In the 2012 book *Web of Deceit*,[120] Mintz attempts to fill the gap in our understanding of cybercrime and the social media,

[116] Kizza, J. and Kizza, M.F. (2008) Securing the Information Infrastructure. London: Cybertech Publishing.
[117] Moore, R (2011) (second edition) Cybercrime: Investigating High-technology Computer Crime. Burlington: Anderson Publishing.
[118] Reveron, D. (2012) (ed.) Cyberspace and National Security. Washington: Georgetown University Press.
[119] Awan, I. Bleakemore, B. (2012) (eds.) Policing Cyber Hate, Cyber Threats and Cyber Terrorism. Farnham: Ashgate.
[120] Mintz, A. (2012) (ed.) Web of Deceit: Misinformation and Manipulation in the Age of Social Media. New Jersey: Information Today, Inc.

while Holt's 2013 book, *Crime on-Line*,[121] provides an overview of various topics on cybercrime, including Internet e-mail scam 'frauds'. Holt also provides a rare qualitative study of the policing of computer crime in the US. Some of issues he touches on include police resources, training and capability, which I will also examine in this thesis.

Rod Broadhurst and Lennon Chang's 2013 book, *Cybercrime in Asia: Trends and Challenges*,[122] focuses, as the title suggests, specifically on Asia. The book provides a brief survey of cybercrime in the Asia Pacific region, especially the problems posed by cloud computing and social media. Broadhurst and Chang conclude that there is no easy answer or solution to the problem of computer related crime.

Literature on Internet Crime in Hong Kong

Internet crime in Hong Kong, especially economic crime, is an under-researched area, which is interesting given the importance of economic activities to the Hong Kong government and society. Even the Hong Kong Crime Victimisation Survey does not cover the victims of white collar crime. Initiatives in this area tend to come from government agencies and the Law Reform Commission.

In 2000, Chan's unpublished thesis, *A comparative study of reported and unreported computer crimes*,[123] specifically examines why computer crime tends

[121] Holt, T.J. (2013) (Second Edition) (ed.) Crime On-line: Correlates, Causes, and Context. Durham: Carolina Academic Press.
[122] Broadhurst, R. Chang, L.Y.C. (2013) 'Cybercrime in Asia: Trends and Challenges', in Liu, J.H. Hebenton, B. and Jou, S. (eds.) Handbook of Asian Criminology. London: Springer.
[123] Chan, Hilton Kwok Hung (2000) A comparative study of reported and unreported computer crimes, Unpublished PhD Thesis, Hong Kong University of Science and Technology. Hong Kong.

to be unreported and what factors would encourage more reporting. He concludes that it is extremely difficult for researchers to directly access research data on the topic, which is a problem that I also share in this thesis.

In 2005, K C Wong's *Discovery of Computer Crime in Hong Kong*[124] and Yiu Chung Lau's *Governance in the Digital Age*[125] both touch on the issue of cybercrime in Hong Kong, although neither study looks at the policing of Internet banking fraud. Lau examines the governance of the Internet in Hong Kong, while Wong focuses on the origin of the Hong Kong police force's approach to policing of the Internet. In *The Politics of Cross-Border Crime in Greater China*, Sunny Lo[126] briefly touches on the issue of Internet crime as a trans-border crime. In his, *Cybercrime in the Greater China Region*, Lennon Chang[127] does not specifically address the development of cybercrime in Hong Kong, as his book focuses more on the crime that occurs between Taiwan and mainland China. Chang points out that despite their difficult political situation, Taiwan and mainland China's still have a good working relationship in policing Internet crime. In this thesis, I also explore whether the close economic and political integration between Hong Kong and mainland China has also led to a closer working relationship in regard to cross-border Internet crime.

[124] Wong, K. C. (2005) 'The Discovery of Computer Crime in Hong Kong: A Case Study of the Crime Creation Process' JILT 2005 (1). Website: < http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_1/wong/>.
[125] Lau, L.Y.C. (2005) 'Governance in the Digital Age: Policing the Internet in Hong Kong'. In Broadhurst, R. and Grabosky, P. (eds.) Cyber-Crime: The Challenge in Asia. Hong Kong: Hong Kong University Press.
[126] Lo, S.S.H. (2009) The Politics of Cross-Border Crime in Greater China: Case Studies of mainland China, Hong Kong, and Macao. New York: East Gate.
[127] Chang, L.Y.C. (2012) Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait. Cheltenham: Edward Elgar Publishing.

Literature on Banking Fraud

As with other forms of economic crime, the literature on fraud and banking-related economic crime mostly focuses on the US and the UK. For example, Michael Levi's 1987 book, *Regulating Fraud*,[128] provides a detailed overview of how fraud is committed by the 'upper-world' and how it is regulated in the UK context. In his 1999 book, *Fraud: Organisation, Motivation and Control*[129], Levi collects some of the best journal articles from different scholars around the world to provide an informative summary of the development and regulation of fraud.

Robb's 1992 book, *White-Collar Crime in Modern England*,[130] provides insight into how the newly industrialised England of the 1840s and 1920s changed the business environment, as big business came to be dominated by large, joint-stock companies, which offered greater opportunities for criminal exploitation. He shows how bankers, stockbrokers and company directors colluded to commit traditional financial fraud. Robb's research gives us some idea of how changes in the wider business environment can affect the opportunities for committing fraud. In the twentieth century another kind of change, the introduction of the Internet, has also brought radical changes to the banking landscape, not least between Hong Kong and mainland China. In this thesis, I explore whether this has brought more opportunities to commit crimes such as Internet banking fraud.

[128] Levi, M. (1987) Regulating Fraud: White-collar Crime and the Criminal Process. London: Tavistock Publications.
[129] Levi, M. (1999) Fraud: Organisation, Motivation and Control II. Aldershot: Dartmouth Publishing.
[130] Robb, G. (1992) White-Collar Crime in Modern England. Cambridge: Cambridge University Press.

Goldmann's 2010 book, *Fraud in the Markets,*[131] provides an overview of how complex factors, such as sub-prime mortgages, almost brought the US financial system to the point of collapse in 2007. Goldmann explicitly names some of Wall Street's top bankers and stock traders as having engaged in fraudulent practices, who he describes as the 'enemies within' the financial system. In 2010, Davies's *The Financial Crisis*[132] and in 2011, Lendman's *How Wall Street Fleeces America*[133] both echo Goldmann, although Lendman goes further and provides an insight into how the bankers elevated themselves to become the most powerful people in the financial world, accountable to no government.

Turner's 2011 book, *Money Laundering Prevention*[134] provides an overview of how anti-money-laundering tools have helped prevent money laundering. Turner sees money laundering as the epitome of fraud. Internet banking can be used as a tool for money laundering by funnelling fraudulent funds from the host country to other countries. In this thesis, I touch on this issue in regards to the transfer of funds between mainland China and Hong Kong after 1997.

Ryder's 2011 book *Financial Crime in the 21st Century*[135] offers an in-depth analysis of fraud and the corresponding governmental policies and regulatory mechanisms in the UK. Ryder focuses on how these regulatory policies have been implemented in the UK and the US. In his 2012 article, *States, Frauds, and*

[131] Goldmann, P. (2010) Fraud in the Markets. New Jersey: John Willey & Son.
[132] Davies, H. The Financial Crisis: Who is to Blame? Cambridge: Polity Press.
[133] Lendman, S. How Wall Street Fleeces America. Atlanta: Clarity Press.
[134] Turner, J.E. Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud. New Jersey: John Wiley & Son.
[135] Ryder, N. (2011) Financial Crime in the 21st Century. Northampton: Edward Elgar Publishing Ltd.

*the threat of Transnational Organized Crime*,[136] Levi concludes that fraud and corruption are very serious threats to some nations and harmful to all. However, he argues that socio-legal and criminological scholars in the US and the UK do not see this kind crime as connected to transnational organised crime. This type of financial crime is, he says, intertwined, transnational and converges with both organised crime and 'white-collar crime'. By design or by accident, the police often label financial crime as two separate types, i.e. 'organised crime' or 'white-collar crime', thus making it very difficult to identify it as one distinctive type of transnational organised crime.

In Frankel's 2012 book, *The Ponzi Scheme Puzzle*[137] provides an historical overview of a type of fraud intertwined with banking fraud, such as the Ponzi scheme. The term 'Ponzi scheme' is often used to describe schemes that involves complex layers of people, where the top promoter has considerable control over every facet of the scheme, including when to terminate it. Internet banking fraud also often involves a similarly interlocking and sophisticated layering of technologies, people and accounts, which are often trans-border.

Literature on Banking Fraud in Hong Kong

There are few existing studies on banking law and regulations in Hong Kong. In their 2000 book, *Financial Regulation in the Greater China Area*, Norton et al.[138] examine banking regulations and the law. In their article 'Assessing anti-phishing

[136] Levi, M. (2012) 'States, Frauds, and the threat of Transnational Organized Crime' *Journal of International Affairs*, Fall/Winter. Vol. 66, No. 1.
[137] Frankel, T. (2012) The Ponzi Scheme Puzzle: A History and Analysis of Con Artists and Victims. Oxford: Oxford University Press.
[138] Norton, J. J., Li, C.J, Huang. Y. (eds.) (2000) Financial Regulation in the Greater China Area: Mainland China, Taiwan and Hong Kong SAR. The Hugue: Kluwer Law International.

preparedness', Bose and Leung[139] examine phishing as a particular type of fraudulent activity and conclude that some of the banks in Hong Kong are better prepared than others in terms of their anti-phishing measures.

Given the lack of literature in this field, this thesis provides a valuable addition to our limited understanding of Internet banking fraud in Hong Kong. Although the thesis does not provide a complete picture of the topic, it does fill some of the gaps in our knowledge of Internet crime, how it has changed since 1997 and how wider changes in society affect how the police and other agencies deal with the crime in its widest sense. I also attempt to explain how and why the investigation of Internet crime has become so important.

Fieldwork

I conducted empirical to discover how the banks, police and courts deal with Internet banking fraud. I looked at:

1) what is meant by Internet banking fraud;
2) how it is reported, recorded and investigated by the banks, the police and other criminal justice agencies, and tried by the courts; and
3) how the crime and its investigation is shaped by the culture, economy, politics and laws in Hong Kong, and the process of 'mainlandisation' since 1997.

[139] Bose, I. Leung, A.C.M. (2008) 'Assessing anti-phishing preparedness: A study of online banks in Hong Kong'. Decision Support Systems 45.

Interviews

The primary data used in this thesis were generated from taped semi-structured interviews with staff from six organisations in Hong Kong: (i) the Hong Kong Police, (ii) a major international bank, (iii) a major international credit card company, (iv) a medium size local Chinese bank, (v) a major international management consultancy firm and (vi) the Department of Justice. I gained access to these organisations through personal contacts. In total, 10 interviews were conducted at their offices, which on average lasted 2 to 2 ½ hours each. The respondents were selected because their day-to-day work involves the prevention, detection and investigation of Internet banking fraud.

The four respondents from the banks included:

(i) a manager of Internet banking within a global bank;
(ii) a manager of Internet banking within a local bank;
(iii) a director of credit card security within a global credit card company; and
(iv) a regional director of the forensics investigation section within a major international consultancy company.

The participants were all senior figures working within major firms in Hong Kong, with knowledge and experience of how these firms handled Internet economic crimes.

The interviewees from the Hong Kong police included:

(i) the head of the Technology Crime Department (TCD) – a senior Superintendent with 26 years' experience of policing in Hong Kong;

(ii) a deputy head of the TCD – a superintendent with 20 years' experience of policing in Hong Kong and a PhD in Internet security;
(iii) a chief inspector of the TCD – with over 20 years' experience of policing in Hong Kong and a degree in engineering;
(iv) a sergeant of the TCD – with over ten years' experience of policing in Hong Kong;
(v) a frontline constable of the TCD – who has been in this division for about 2 years.

One respondent was interviewed from the Department of Justice. The respondent was a qualified barrister working in a section specialising in advising and prosecuting computer crimes (set up in 2000). These prosecutors attended local and overseas courses on how to handle and understand digital evidence and share experience with overseas prosecutors.

Prior to each semi-structured interview, I explained the aims of my research. I also informed the participants of their right to refuse my request for an interview. They all volunteered to take part. Before the semi-structured interviews began, I always informed the participants that the information disclosed in the interviews would remain anonymous. I stored all the recorded interview tapes and transcripts in a private study room, which was locked.

The semi-structured interview tapes were transcribed. Some of the interviews with the police officers in Hong Kong were conducted in Chinese. These were subsequently transcribed and translated into English.

The Case Sample

In addition to the interviews, I analysed fifteen cases involving Internet economic crimes that were prosecuted under the Computer Crimes Ordinance 1993. These cases occurred between 1999 and 2012, and were taken from reports of cases of Internet crimes that were tried and went to appeal in Hong Kong. This means that the cases were ***reported*** cases, i.e. the cases were reported in the Law Reports and went to the Court of Appeal. It is not possible to determine the total number of cases arising in this period, as other cases may have (i) been reported to the authorities but later dropped; (ii) ended in a plea of guilty before trial; or (iii) gone to trial but not been reported in the Law Reports. The cases dealt with here are those that went appeal. As reported appeal court cases, they are seen as potentially precedent-setting cases of some importance. They are also more readily available to the researcher, as unreported cases are not accessible to parties not directly involved in the cases. No direct courtroom observation of cases was conducted. Although the sample is small (15 cases), it includes the major cases in this area during this period. For example, one of the cases involved the first prosecution and conviction for insider dealing in Hong Kong. Another involved a senior manager of a well-known Chinese listed bank in Hong Kong who was convicted of conspiracy to defraud. Both these cases were highly publicised. Another, involving allegations about a senior political figure in Hong Kong, also received much publicity.

The cases are as follows.

*Case 1: HKSAR v Tsun Shui Lun-[1999] 2 HKC 547, Magistracy Appeal No 723 of 1998*

*Case 2: HKSAR v Tam Hei Lun & ORS-[2000] 3 HKC 745, Magistracy Appeal No 385 of 2000*
*Case 3: HKSAR v Choy Yau Pun-[2002] 4 HKC 309, Magistracy Appeal No 450 of 2002*
*Case 4: HKSAR v Lai Mei Yuk [2004], Criminal Appeal No 427 of 2003*
*Case 5: RE Chen Kam Chiu and Others-[2005] HKCU 987, CACC 179/2004 (On Appeal HCCC No 158 of 2003)*
*Case 6: Chiu Hoi Po v Commissioner of Police-[2006] HKCU 681, HCAL 105/2003*
*Case 7: HKSAR v Leong Wai Keong-[2008] HKCU 1915, Court of Appeal CACC 476/2007*
*Case 8: HKSAR v Kam To Fung-[2008] HKEC 1041, Magistracy Appeal No 565 of 2007*
*Case 9: HKSAR v Marimuthu Jaisanka-[2008] HKCU 243, Court of Appeal CACC 403/2007*
*Case 10: HKSAR v Ho Ching Wah-[2009], Court of Appeal CACC 106/2008*
*Case 11: HKSAR v Ma Hon Kit Sammy & ORS-[2010] HKCU 2189, Court of Appeal CACC 148/2009*
*Case 12: HKSAR v Cai Zhaorong-[2012], Court of Appeal CACC 365/2011*
*Case 13: HKSAR v Chan Wai Ming-[2012] DCCC 137B/2011*
*Case 14: HKSAR v Cheung Yiu Ming-[2012] DCCC 320/2011*
*Case 15: HKSAR v Yaghi Jose-[2012] DCCC 141/2012*

All but one these cases went to trial and led to conviction. The case that did not was an internal police disciplinary tribunal that went to judicial review.

In analysing these cases, I follow the methodology established by T. Wing Lo and Paul Ngan in their 2009 article published in *Crime, Law and Social Change*[140] to find any evidence of whether and how any of the cases have been affected by any of the factors listed in Chapter One.

Access

A question for researchers is how to gain access to the institutions and groups being studied. In this case, this meant gaining access to banks, the police and the

[140] T. Wing Lo, Paul Ngan, (2009) 'Restricting Loans of Money to Hong Kong Civil Servants: Social censure or Violation of Human Rights?' Crime, Law and Social Change, Springer 52, pp. 385-403.

Department of Justice. These institutions are well-known to socio-legal and criminological researchers as being difficult to gain access to, as they are powerful and secretive. As Hornsby-Smith says:

> "*It is far more difficult to study powerful individual and bureaucracies…because elites and powerful people and institutions are frequently able to deny access because they do not wish themselves or their decision-making process to be studied…*"[141]

Researchers typically experience problems gaining access to such groups. As Chan mentions, "*it is extremely difficult for outside researchers to have any direct access whatsoever to the research data for analysis*".[142] In her study on surgeons, Joan Cassell[143] spent over a year trying to access her research subjects before gaining it through a chief surgeon who was a friend of her ex-husband. Likewise, I was only able to gain access to the police through a personal friend who held a senior position in the Hong Kong government. After I had spent months trying to gain access, my friend personally spoke to the Commissioner of Police on my behalf. Even so, a limit was placed on the number of serving police officers I could interview and conditions were placed on the time and date of the interviews.

Limitations

The problems I encountered gaining access to the Hong Kong police without any formal or official status highlighted the fact that I am what Reiner and Newburn call an 'outsider outsider':

---

[141] Hornsby-Smith, M. (1993) 'Gaining Access', in Gilbert, N. (ed.) Researching Social Life, London: Sage, p. 53.
[142] Chan, Hilton Kwok Hung (2000) Ibid.
[143] See Cassell, J. (1988) 'The Relationship of Observe to Observed when Studying Pp,' in Burgess, R. G. (ed.), Studies in Qualitative Methodology, London : JAI Press.

> "*Outsider outsiders clearly face the greatest barriers in gaining formal access to police forces for research. They have no official status that mandates formal police co-operation and may (often rightly) be perceived as having critical concerns about police malpractice or failure…Negotiating access usually involves more than one hurdle. The extent of difficulty will vary from time to time according to the political climate of the police elite…*"[144]

It was also difficult to gain access to the official statistics on Internet economic crimes, partly because of the lack of accurate and specific figures on this kind of crime in the public domain, and also because of the lack of research in this area. Even if the figures do exist, they remain difficult to access and questions remain about how much they can be relied upon.

There are also other limitations. For example, the interview schedules were semi-structured and possibly open to unconscious bias in the manner in which the questions were asked. In addition, there is always a danger that the interviewees will not answer the questions fully.

As a result, the picture I paint in this study may only tell part of the story. Despite these shortcomings, this is the first empirical study of how the banks, police and courts handle Internet banking fraud in Hong Kong.

[144] Reiner, R. and Newburn, T. (2008) Ibid. p. 357.

# Chapter Three
# Technological and Financial Savviness

## Introduction

In this chapter, I discuss how Hong Kong society provides a particular context for the investigation of Internet crime, particularly Internet economic crime (in this case, Internet banking fraud). As mentioned in Chapter One, my main focus is the technological and financial 'savviness' of the local population, as manifest in their rapid take-up of the latest technology and their knowledge and use of technology for economic transactions. I suggest that the technological and financial know-how of the Hong Kong population is culturally distinctive. In this chapter, I document the nature and extent of this local culture, and the importance of economic and technological 'savviness' in everyday Hong Kong life.

In part, the cultural acceptance of finance and technology in Hong Kong is shaped by the fact that many of the early migrants were refugees, for whom political insecurity meant that 'cash is king'. In part, this cultural disposition is due to Hong Kong's history as a trading city, an export economy and a vital channel for mainland China to earn foreign exchange during the Maoist period. Money and commerce have long flowed inwards in Hong Kong, from the Chinese diaspora and through international finance and commerce, but also outwards, towards the rest of the world and across the frontier with China.

Hong Kong's culture and history, and the importance of financial transactions in everyday life, have arguably made Hong Kong particularly receptive to the uptake of Internet banking. The heightened awareness of technology and the

centrality of 'money consciousness' in Hong Kong has directly contributed to the widespread use of the Internet for economic and banking transactions. At the same time, this has made the local population susceptible to Internet banking fraud. However, Hong Kong's culture and history has also helped shape the way the banks, the police and the courts react to crimes such as Internet banking fraud.

Technological and Financial 'Savviness'

Hong Kong people are generally very technologically and financially savvy. The first Chief Executive of Hong Kong was an engineer, echoing the preference of mainland China for leaders with practical technological skills. Moreover, education is still regarded as ***the*** key to social mobility in Hong Kong. There is a deeply embedded cultural belief that education not only broadens the mind, but also translates into wealth. Andreas Schleicher, the coordinator of the OECD's highly-influential Pisa tests, states that in Chinese society *"the idea is so deeply rooted that education is the key to mobility and success*".[145] In Hong Kong, the Chinese University of Hong Kong, University of Hong Kong, City University of Hong Kong and University of Science and Technology are all ranked within the top 100 universities in the world.

According to Henderson, in the 1960s Hong Kong was already emerging as a regional centre for high-tech semi-conductor manufacturing.[146] By the late 1980s, there were 21 semi-conductor companies in Hong Kong. The fact some of these

[145] See Coughlan, S. (8 May 2012) 'China: The World's Cleverest Country?' BBC News Online. [Online] [Visited 10/5/2012], at: <http://www.bbc.co.uk/news/business-17585201>.
[146] Henderson, J. (1989) The Globalisation of High Technology Production: Society, Space, and Semiconductor in Making of the Modern World. London: Routledge, p. 96.

companies were carrying out research and development is a clear sign that Hong Kong possessed the capacity for technological innovation. As Henderson says:

> "*Three of the US companies (Motorola, Siliconix, and Zilog) have design centres in Hong Kong. Motorola's design centre is one of its three largest outside of the United States, Siliconix's is a joint venture operation with an independent Hong Kong-owned design house (Central Systems Design), and Zilog's design centre is its only productive operation in the territory and complements its Asian regional headquarters, which is also located in Hong Kong*."[147]

Furthermore, in the 1980s people in Hong Kong preferred to use radio personal pagers for personal and business communications. As a result, Hong Kong's radio personal pager technologies were the most advanced in Asia. By the late 1980s, Hong Kong society had already started to move away from personal pagers to first generation mobile telephones. In 1993, the world's first commercialised digital telephone technology was introduced in Hong Kong[148].

In the 1990s, Hong Kong briefly experimented with the computer software industry. The structural change from a manufacturing to a services based economy created a demand for technological products to service the growing needs of the customer based industries. Furthermore, as a result of globalisation, Hong Kong needed to become more technologically advanced to retain a competitive edge over its Asian trading rivals. As a result, in 1993, Hong Kong's

[147] Henderson, J. (1989) Op Cit.: p.112.

[148] An operating licence was granted to a mobile phone company called 'SmarTone', which used a Global System for Mobile communication technology (GSM). This GSM technology enabled mobile telephone communications underground (inside the Mass Transit Railway (MTR)and all the road tunnels and cross-harbour tunnels in Hong Kong). In contrast, in the UK, even in 2009, the London underground still failed to provide mobile-phone communication services in train carriages inside the tunnel.

total IT market was valued at around US$837 million, of which trade in hardware accounted for 67 per cent, while software only contributed 12 per cent.[149] By 1995, according to a government commissioned study, there were approximately 500 independent software vendors (ISVs) in Hong Kong, employing a total of 8,500 personnel.[150] The majority of these ISVs were small-medium size firms with 20 or fewer employees. Most of them were in the custom software business, offering software solutions to support industries such as manufacturing and finance.[151]

In the late 1990s, the emergence of the Internet provided the basis for another IT-related industry in Hong Kong. However, the Internet fever vanished within 18 months. Then, the 1997 Asian financial crisis (from 1997 until mid-2004) forced a rethink of the value of the creative industries. The Hong Kong government initiated a number of programmes to promote technology and to try to move Hong Kong's economic framework from a traditional base to a modern knowledge base. One initiative was to provide state-of-the-art infrastructure to create a strategic information technology cluster. In his inaugural speech as Chief Executive in 1 July 1997, Tung Chee-Hwa declared that the foremost task of his government was to enhance Hong Kong's economic vitality and growth. Tung's message was that he wanted to transform Hong Kong into a knowledge-based

[149] See the Hong Kong Government Industry Department. (1994-5) Consultancy Study on Hong Kong's Software Industry (Phase II Study - Market and Technology Trend Analysis). Hong Kong: Hong Kong Government Printer.
[150] Hong Kong Government Industry Department. (1994-5) Ibid.
[151] However, according to Berger and Lester, there was little future in offering such packaged software, because such development relies heavily on research and development, 'creative genius' and sophisticated marketing support. See Berger, S., Lester, R. (eds.) (1997) Made by Hong Kong. Hong Kong: Oxford University Press, pp. 238-243.This kind of short-termism (developing software 'for a quick kill') worked for a while. However, the software development industry perished by the mid-1990s.

economy centred on information technology and to overcome the region's dependence on finance and real estate to a knowledge-based economy, especially information technology.[152] He promised, for example, to create a 'Cyberport' and 'Science Parks':

> *"There is no question that, for Hong Kong to meet the challenges of the 21st Century, it must adapt to new forces of the Information Age….To respond to these mega trends…We should exploit the strengths of our sophisticated telecommunications network……give Hong Kong an edge in developing information services…With these considerations in mind, the Government proposes to develop a "Cyberport" in Hong Kong. The Cyberport will provide the essential infrastructure for the formation of a strategic cluster of information services companies."*[153]

In 2001, the government also established a science park near Tai Po to advance innovation and technology. Covering an area of 22 hectares, the park provided 20 state-of-the-art laboratory-fitted buildings and 220,000 square metres of office space.[154] The aim of the park was to drive the development of electronics, information technology, telecommunications, biotechnology and precision engineering.[155] The government wished to turn Hong Kong into a leading information technology hub and digital city in the Asia-Pacific region by developing a hi-tech economy and attracting international technology organisations to set up research and development operations in the hi-tech science

[152] Lau, S.K. (2002) Op Cit.: p.7.

[153] 3 March 1999, The Financial Secretary, Donald Tsang, The 1999-2000 Budget: Onward with New Strengths. Hong Kong: Hong Kong Government, para.57-8, p.15. The Cyberport was a US$2 billion (HK$15.8 billion) landmark project managed by Hong Kong Cyberport Management Company Limited, which is wholly owned by the Hong Kong Government. It hoped to attract quality information technology and related companies to set up regional offices in Hong Kong.

[154] Hong Kong Science Parks. (2008) Hong Kong Science Technology Parks Annual report 2007/2008, p.2.

[155] The Science Park consists of a number of sites. The aim of the park is to provide infrastructure and subsidised office space to enable technology-related businesses to conduct research and development.

parks. In turn, the international organisations were expected to nurture local IT talent. In October 2002, Microsoft moved its entire operations for greater China (including software research and development) to Hong Kong Cyberport.[156]

Today, the technological advancement in China is linked to the country's economic development and increasing purchasing power. After being re-integrated with China inafter 1997, Hong Kong has becme increasingly linked to China's economic advancement. This has enabled Hong Kong to skip a generation of technological development and to directly acquire the latest modern technology, and placed a new emphasis on the need for technological knowhow.

With the introduction of new technologies (such as mobile communications) and the increase in purchasing power, Hong Kong people have become increasingly technologically literate. More and more people use their Internet accounts to conduct daily banking activities, such as paying bill and transferring funds, sometimes across continents. A large number of people also use their online banking account to buy and sell stocks and shares on a daily basis. In July 2009, in the midst of a global financial crisis, Kwok observed that:

> "*Another Hong Kong IPO mania is in the making. Beijing's largest cement supplier BBMG Corp on Thursday raised $768 million in an initial public offering*

[156] Microsoft Hong Kong Ltd. [online] [cited 14/08/2009]. Available from: <http156 S://www.microsoft.com/hk/mscorp/backgrounder.mspx>. By the mid-2000s, several specialist computer-generated imagery (CGI) animation studios, which make animation movies for Hollywood, had set up production and research and development operations in Hong Kong. As Lewis states, "*Hong Kong, is stepping into the limelight as the engine of Asian computer-generated imagery (CGI) animation and not merely because movie production costs a third of what it would in California. Hong Kong, unlike Japan, has an unlimited supply of young, creative and technologically literate people ready to turn the island into an animation hub"*. See Lewis, L. (February 23, 2008) 'Out-ward looking Hong Kong hopes to capture Asian animation crown'. London: The Times. [Online] [Cited 15/08/2009]. Available from: <http://business.timesonline.co.uk/tol/business/markets/china/article3419338.ece>.

> *in Hong Kong. BBMG's new shares were 770 times oversubscribed by retail investors. How to get hold of the hot shares of BBMG was the most popular topic for phone-in radio programs and financial news portals in Hong Kong over the past week. Thanks to the substantial demand, state-owned BBMG Corp. priced its IPO at 6.38 Hong Kong dollars (82 cents) per share, the top end of an indicated range between 5.18 and 6.38 Hong Kong dollars (66-82 cents.). BBMG's 770-time oversubscription from individual investors even broke the record of BaWang, the popular Chinese shampoo maker which used Kung Fu star Jackie Chan to promote its herbal shampoo on TV round the clock. BaWang's IPO last month attracted 446-times-oversubscription"*[157]

In addition, one reason for this financial savviness is that the Hong Kong government provides little welfare for people when they fall on hard times. Cash is the only security that people can rely on. The government has to be seen to provide protection for people's hard earned money and their savings. Moreover, as ordinary people also tend to chase fast profits, they frequently use their online banking accounts to buy and sell shares. For example, in October 2006, the applications for the initial public offering (IPO) of the Industrial and Commercial Bank of China (ICBC) in Hong Kong were 100 times over-subscribed, with around one million people applying for the shares. According to Froster and Tang, empirical data show that Internet purchases for banking and financial services in Hong Kong reached 26 per cent in 2003 (Feb-June).[158]

---

[157] Kwok, V.W.Y. (07.23.2009) 'IPO Fever Hits Hong Kong'. Hong Kong: Market Scan (Forbes.com). [online] [cited 28/07/2009]. Available from: <http://www.forbes.com/2009/07/23/hk-ipo-boom-markets-equity-china_print.html>.

[158] Froster, P.W., Tang, Y. (2005) 'The Role of Online Shopping and Fulfillment in the Hong Kong SARS Crisis'. Hawaii: Proceedings of the 38th Hawaii International Conference on System Sciences, Table 1, p.3. As Froster and Tang state, "*By June most sectors had dropped with the notable exception of banking and travel. While clearly the increase in travel was directly related to the lifting of the WHO travel advisory, the rise in banking and other sectors raises the question whether online behaviour was permanently changed by the SARS experience*."

There is also a strong cultural bias towards science, engineering and technology subjects in Hong Kong. Because officers are recruited from this technologically and financially literate population, the police in Hong Kong are therefore familiar with the technology of Internet banking fraud. As Table 3.1 shows, in 2007/2008, twice as many students were enrolled in science and technology degrees than arts and humanities (66.46 per cent and 33.54 per cent, respectively).

**Table 3.1: University Student Enrolment in Hong Kong (University Grants Committee (UGC) Funded Degree Courses), 2007/2008**

| Institutions | Science, Technology, Computer, Maths and Engineering related subjects | Arts and Humanities related subjects | Total |
|---|---|---|---|
| **City University (CityU)** | 7092 | 2441 | |
| **Baptist University (BU)** | 2056 | 3028 | |
| **Lingnan University (LU)** | 802 | 1539 | |
| **Hong Kong Institute of Education (HKIEd)** | 510 | 3588 | |
| **Polytechnic University (PolyU)** | 11125 | 1695 | |
| **University Science and Technology (HKUST)** | 6531 | 277 | |
| **Chinese University (CU)** | 7991 | 4670 | |
| **Hong Kong University (HKU)** | 7824 | 4928 | |
| **Total** | 43,931 | 22,166 | |
| **Percentage** | **66.46%** | **33.54%** | |

*(Sources: University Grants Committee Statistic (Student Numbers) 2007/08. [Online] [Cited 13 /08/2009]. Available from: <http://www.ugc.edu.hk/eng/doc/ugc/stat/heiapcfte2.pdf>).*

Since the 1990s, Hong Kong has become even more technologically advanced. This has led to the development of a number of new industries and the expansion of the existing telecommunications and computer-related industries. The

deregulation of the telecommunications industry in the late 1980s opened the market to competition. New-comers joined the race and gradually helped build Hong Kong's telecommunications infrastructure, pushing down the price of local and international telephone calls.[159] By 1993, the territory had developed an advanced telecommunication infra-structure, based on fibre optics. Telephone coverage reached 60 per cent, and the mobile phone penetration, at 16 per cent, was the highest in Asia at the time. By March 2000, mobile phone penetration had jumped to more than 52 per cent, upholding Hong Kong's number one position in Asia. In June 2005, there were 8,384.880 mobile phone subscribers, representing 120.8 per cent penetration, with 1,618,656 subscribers connected to 2.5 and third generation mobile technologies.[160] By 2000, there were at least half a dozen companies that provided international telephone services, six licenced service providers for mobile phones and approximately 184 ISPs. The rapid growth of these IT-related industries was partly due to Hong Kong's affluence and its receptiveness to anything new. The fast take-up of third generation mobile technology is a case in point.

Hong Kong's technological advancement is supported by the World Bank's World Development Indicators (see Table 3.2 below), which show that between 2005 and 2006, there were 2,650 researchers and 341 technicians in R&D per

[159] Ure, J. (2008) 'Hong Kong', in Ure, J. (ed.) Telecommunications Development in Asia. Hong Kong: Hong Kong University Press, pp. 180-183.
[160] See the Office of the Telecommunication Authority [Online] [Cited 27/09/05]. Available from: <http://www.ofta.gov.hk/en/datastat/key_stat.html>. By the 2011, the figure rose to 7.45 million subscribers for 3G mobile-phone service.

million population in Hong Kong, and that expenditure for R&D (% GDP) rose from 0.7% to 0.81%.[161]

**Table 3.2 Indicators of Technological Development**

| Country | Researchers in R&D per million people (2006) | Technicians in R&D per million people (2005) | Scientific and technical journal articles (2006) | Expenditure for R&D (%GDP) (2006) |
|---|---|---|---|---|
| Japan | 5'568 | 563 | 54'456 | 3.40 |
| Hong Kong SAR | 2'650 | 341 | N/A | 0.81 |
| South Korea | 4'187 | 552 | 17'910 | 3.01 |
| Singapore | 5'736 | 557 | 3'838 | 2.27 |
| China | 927 | N/A | 49'575 | 1.42 |

*(Source: The World Bank, World Development Indicators, website: http://data.worldbank.org/indicator).*

In the late 1990s, Hong Kong witnessed the phenomenal growth of the Internet. However, the industry went through a boom and bust cycle within the space of 18 months. In 2000, the Office of the Telecommunications Authority[162] reported that there were almost 400 registered ISPs in Hong Kong. However, by August 2005, only 184 registered ISPs remained. Despite the collapse of the Internet industry, its development left Hong Kong with one of the best Internet infrastructures in the world. The Internet usage rate in Hong Kong is much higher than in most other industrialised countries, with 99 per cent of households having access to broadband networks and 68 per cent of households using broadband services.

Of significance to this thesis, the number of people using Internet banking also rose, from 1.1 million personal online bank accounts in 2001 to 3.6 million by

[161] The computer software industry was also largely fuelled by the structural change in the Hong Kong economy from a manufacturing to a service base. There was a demand for technological products to service the growing needs of the customer-based industries, such as Hong Kong's financial sector and the vibrant textile design industry, which for example, drove the local software company, 'Prima Design Systems', to become a pioneer in utilising colour CAD systems for textile and garment design.

[162] See Hong Kong Office of the Telecommunications Authority. [Online] [Cited 28/09/05]. Available from: <http://www.ofta.gov.hk/en/datastat/key_stat.html>.

mid-2006,[163] the latter figure representing 53 per cent of the total population.[164] Moreover, as Table 3.3 shows, in 2009, Hong Kong was ranked 12th in the world in terms of information technology readiness, 11th in global competitiveness, 21st in technology readiness and 8th in technology usage.

**Table 3.3: Hong Kong's Ranking on Information Technology Readiness in 2009**

| Hong Kong | World Ranking | UK | World Ranking |
|---|---|---|---|
| Technology Networked Readiness | **12** | Technology Networked Readiness | **15** |
| Global Competitiveness | **11** | Global Competitiveness | **12** |
| Society Readiness | **21** | Society Readiness | **24** |
| Society Usage | **8** | Society Usage | **13** |

*(Source: Dutta, S., Mia, I. (2009) Global Information Technology Report 2008-2009. Geneva: World Economic Forum, INSEAD, p.xvii, p.199, p.277)*

As these figures indicate, Hong Kong people are generally technologically and financially savvy, and attuned to new technology. They frequently use Internet banking to buy and sell stocks and shares. Arguably, this means that they may be more vulnerable to Internet banking fraud.

Financial Savviness

Mathews et al say that it is often said that Hong Kong people only live for money:

> *"…'People in Hong Kong are interested in money because with everything else uncertain, money is all that you can depend upon'….the world's highest per capita*

[163] Hong Kong Consumer Council. Press Release. Hong Kong: Hong Kong Consumer Council. [Online] [Cited 27/02/07]. Available from: <http://www.consumer.org.hk/website/ws_en/news/press_releases/p36401.html>.

[164] Siu, N.Y.M. and Mou, J.C.W. (2005) 'Measuring Service In Internet Banking: The Case of Hong Kong'. Journal of International Consumer Marketing. Vol. 17(4), p. 100. These figures mean that Hong Kong has a more advanced Internet banking market than Singapore, South Korea and Taiwan.

> *possession of Rolls Royce is not only a measure of Hong Kong's wealth, but more, an indication that most Hong Kong people will not disdain those who flaunt such cars but instead see them as admirable."*[165]

Hong Kong also has a 'savings culture'. The rapid industrialisation from the mid-1950s to the early 1980s not only brought personal wealth and purchasing power, but also inspired hard work and encouraged people save their hard earned money. By using their savings as equity for their small businesses, many people hoped that they too would become multi-millionaires.[166] Making money and spending money are core Hong Kong activities. As Mathews et al say:

> *"Social class in Hong Kong is based, quite nakedly, on money: the richer you are the better. As a colony and a trading port, old Hong Kong never cultivated its gentry's class….contemporary Hong Kong is pragmatic, materialistic and down-to-earth. The rich, given the fact that they have little cultural capital to draw upon…they do not bother creating barriers to entry to upper social class through criteria of taste and cultural distinction. Ordinary people…remain materialistic in their concerns and world-view…the rich can socially confirm their privileged positions by spending…conspicuous consumption."* [167]

During various periods, large numbers of people have fled to Hong Kong from China because of either civil unrest or famine.[168] Having come to Hong Kong to fulfil their money-making dreams and to search for a better life, these migrants developed an acute sense for making money.

---

[165] Mathews, G., Lui, T. L. (2001) 'Consuming Hong Kong', in Mathews, G., Lui, T. L. (Eds.) Consuming Hong Kong. Hong Kong: Hong Kong University Press, pp.10-11.

[166] In Hong Kong, people are often inspired by the richest businessman in Asia, Li Ka-Shing, who serves as a role model. When he first arrived in Hong Kong from mainland China in the 1950s, Li had only one dollar in his pocket. However, 40 years later, in the 1990s, he had become the 16th wealthiest man in the world.

[167] Mathews et al (2001) Op Cit.: p.8.

[168] In the 20th century, the 1930s civil war between the Communists and the Kuomintang, resumed after the Second World War in 1947 until 1949. According to Tsang, the civil war in China resulted in an influx of refugees crossing the border into Hong Kong. See Tsang, S. (2004) Op Cit.: p.152.

For those who arrived in Hong Kong from China during the 20th century, cash was the most viable and transferable security to be acquired. When they arrived in Hong Kong,[169] these Chinese refugees had no social safety net to support them, which must have heightened their sense of insecurity. Cash was the one tangible object they could hold on to, as it provided security and the ability to flee at a moment's notice. The renewed political uncertainty in the run up to the 1997 transfer of sovereignty reinforced this attitude towards money and saving. In particular, as many people moved overseas, Internet banking was used more frequently as people transferred money back and forth to and from Hong Kong.

Internet banking fraud is therefore more likely to affect these people. Moreover, events such as civil unrest and famine have reinforced the belief in cash, education and savings. However, as the majority of people in Hong Kong use the Internet[170] for their financial transactions, online banking needs to be rigorously monitored by the authorities to prevent the kinds of mass victimization and protest that accompanied that BCCI fiasco.

The BCCI fiasco, other banking scandals and the 1997 Asian financial crisis all showed how the volatility of the financial markets and market malpractice can have widespread effects on the fortunes of ordinary people. These types of

[169] These refugees have witnessed a number of riots in Hong Kong. See Tsang, S. (2004) Op Cit.; Young, J.D. (1994) 'The Building Years: Maintaining a China-Hong Kong-Britain Equilibrium, 1950-71', in Chan, M.K. (ed.) Precarious Balance: Hong Kong between China and Britain, 1842-1992. Hong Kong: Hong Kong University Press, p.139; Cooper, J. (1970) Colony in Conflict: The Hong Kong Disturbances May 1967-January 1968. Hong Kong: Swindon Books.

[170] By 2011, the number of fixed broadband subscribers in Hong Kong reached 2.24 million, see Digital21, The Hong Kong SAR Government, website: < http://www.digital21.gov.hk/eng/statistics/download/informationsociety2012.pdf>. [Visited 22/6/2013].

disturbances also have the potential to harm social stability. To preserve Hong Kong's international reputation, the authorities needed to regulate economic transactions to ensure economic stability and to by keep economic transactions 'clean'. However, according to Milton Friedman, Hong Kong is still a classic case of a laissez-faire capitalist society.[171] Moreover, according to the Index of Economic Freedom compiled by the Heritage Foundation, in 2012 Hong Kong retained its top ranking as the world free-est economy for the 18th consecutive year.[172] As the last colonial governor of Hong Kong, Chris Patten, stated, "*in Hong Kong, Adam Smith held sway in every sort of market*".[173] In theory, therefore, this should mean that banks in Hong Kong are left to police themselves and that they are subject to less government regulation than banks elsewhere. In the following chapters, I examine whether this is the case.

[171] Friedman, M. (October 6, 2006) 'Hong Kong Wrong'. New York: The Wall Street Journal. [Online] [Cited 6/08/2009]. Available from:
< http://online.wsj.com/article/SB116009800068684505.html>.
[172] See the Heritage Foundation. [Online] [Cited 12/01/2012] at:
< http://www.heritage.org/index/>.
[173] Patten, C. (2008) What Next? Surviving the Twenty-First Century. London: Allen Lane, p. 240.

# Chapter Four
# The Bank's Internal Processes of Detecting, Filtering and Reporting Crime

## Introduction

In this chapter will look at how the banks in Hong Kong deal with Internet fraud, including internal processes and decision-making. I also examine whether and how the banks report any instances of Internet fraud to the police and, if not, whether there are other channels for resolving such cases.

## How Banks Process Internet Banking Fraud

There are numerous ways in which banks can deal with Internet banking fraud. For instance, the internal controls within a bank (e.g. internal audits) may bring a crime to the bank's attention. The bank may report the incident to the police or deal with the matter internally. Second, a crime may be detected during an external audit by the Hong Kong Monetary Authority (HKMA), which will then report the crime to the bank or to the police. Third, the victim may report the crime to the bank, the police, the Independent Commission Against Corruption (ICAC) or the Consumer Council (there is no financial services ombudsman in Hong Kong).

Diagram 4A below indicates how fraud comes to the attention of a bank, and the processes whereby the bank either reports the crime to the police or deals with it internally. The diagram also shows that there are a variety of ways in which a bank can deal with a crime before reporting it to the police.

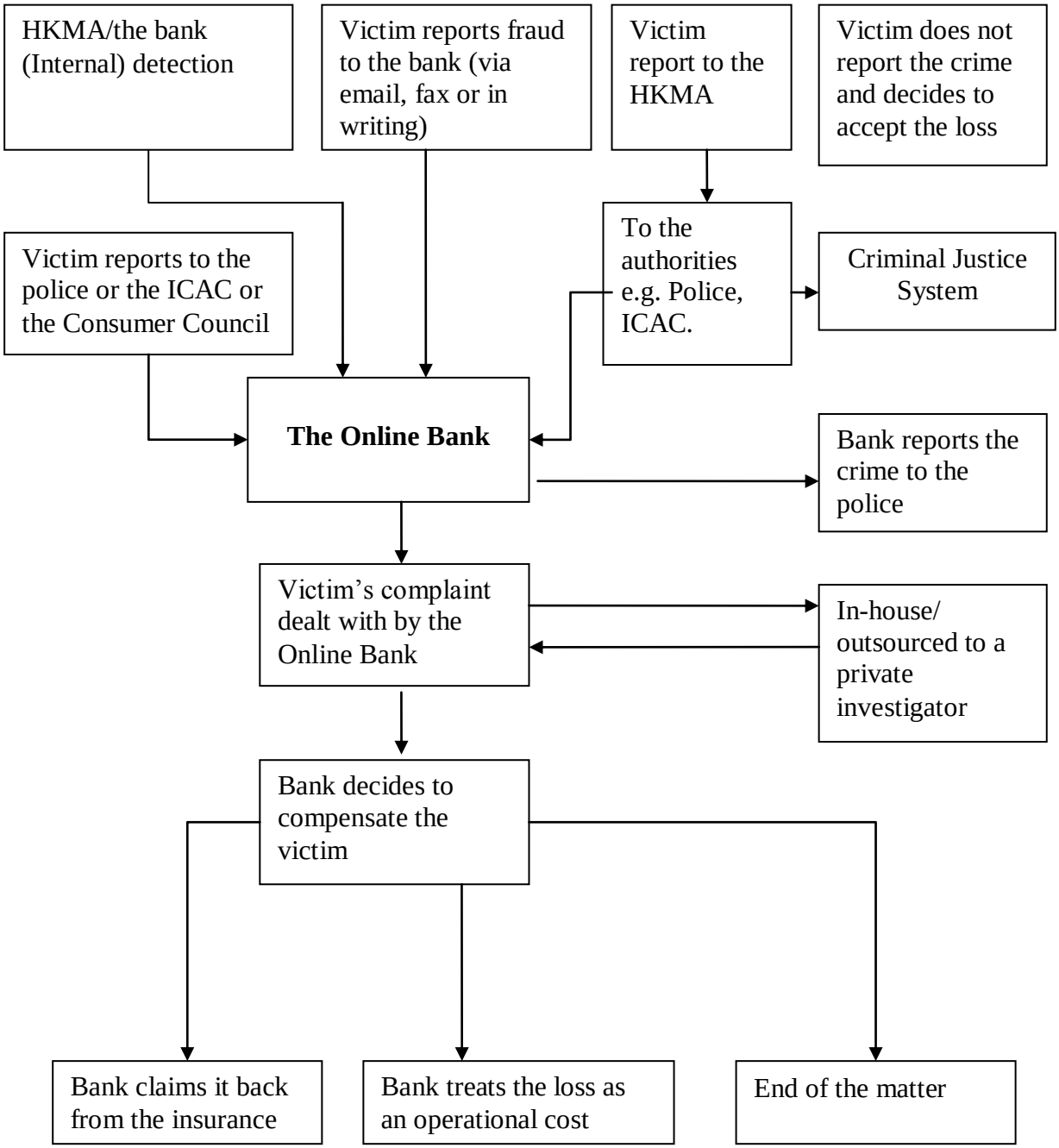



**Diagram 4A: How Banks Process Internet Banking Fraud in Hong Kong**

In an empirical study, Bailey[174] concluded that there *was* unreported computer crime in Hong Kong. However, he did not reach a firm conclusion as to *why* some computer crime went unreported by the victims. Bailey suggested that factors might include the perceived ineffectiveness of the police, that the punishment of computer criminals is seen to be inadequate and the popular belief that computer crime is not commonly reported.

When a case of fraud is reported to a bank, a decision has to be made whether to report the crime to the police. However, a 1993 amendment to the Banking Ordinance stipulates that banks ***must*** [175] report cases of fraud to the HKMA, which will then report them to the police. In cases where crimes have to be reported to the authorities (e.g. to make an insurance claim or to obtain a Hong Kong Identity Card), the literature suggests that the number of reported crimes is likely to be high. However, although the reported crimes become known to the police, they do not enter the official statistics unless the police investigate them and establish the evidence of a crime

Internet Security

One of the main ways of curbing Internet banking fraud is to institute preventative measures. Like their counterparts around the globe, banks in Hong Kong use various types of computer security to protect their customers' bank

[174] Bailey, P.E. (1998) Computer Crime reporting Behaviour: A Hong Kong Study. MA. Thesis (Unpublished). The City University of Hong Kong.

[175] See the Bank Ordinance (Cap.) 155, section 7 (b) (c) (d) (e). This section has empowered the HKMA to perform a number of functions as the supervisor of the banks, including preventing, detecting and reporting fraud to the ICAC or the police. Under section 120 (5) (1) (d) of the Ordinance, the employee will be exempted from the Official Secrecy Act if the HKMA reports fraud to the police.

accounts. In a 2005 survey on information security, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT/CC)[176] found that the information security awareness of organisations in Hong Kong had increased considerably in recent years, with only 3.6 per cent of the organisations surveyed having no information security measures in place. Moreover, the survey also found that a high percentage of the organisations in the banking sector (36.9 per cent) had adopted advanced security technology[177] (e.g. file encryption, access control, intrusion detection systems, virtual private networks, encrypted login, non-reusable passwords, digital IP, public key infrastructure, and biometrics with/without basic security technologies). With regard to computer security management, in addition to using security technologies, a high percentage of organisations in the banking sector (35.7 per cent) have taken proactive measures to improve their computer security by implementing comprehensive information security policies, such as information security risk assessments and audits, incident response procedures and regularly applied security patches.[178] However, in May 2007, in a written reply to a question on the information security survey, the Secretary for Economic Development and Labour formally confirmed that since 2005, the Hong Kong Productivity Council (HKPC) had re-prioritised its activities and categorised the information security survey as a non-core function of the HKCERT/CC, which has since ceased conducting surveys on information

[176] Hong Kong Computer Emergency Response Team Coordination Centre, (March 2005) Information Security Survey 2004, Hong Kong, p. 6.
[177] Hong Kong Computer Emergency Response Team Coordination Centre, (March 2005) Op Cit.: p.11.
[178] Hong Kong Computer Emergency Response Team Coordination Centre, (March 2005) Op Cit.: pp. 20-21.

security in Hong Kong.[179] As a result, any surveys of information security are now conducted by commercial organisations and/or academics in Hong Kong.

In a recent survey on information security awareness, especially in relation to smart mobile-phones, conducted by the City University of Hong Kong and PayPal,[180] 38 percent of the respondents stated that they were concerned about sharing personal information online, while 7 out of 10 stated they used the same password for an average of 7 online accounts. In addition, 60 per cent of those surveyed reported that they never updated their online passwords or only did so when required while over 75 per cent stated they regularly made payments online at least once a month for online shopping and bills. Although Hong Kong people commonly use the Internet to make payments, 78 per cent of the respondents stated that security concerns discouraged them from making more online payments.

Furthermore, in line with the increasing use of smart mobile phones in Hong Kong, over 67 per cent of the respondents stated they preferred to use their mobile phones to make payments because of convenience, efficiency, and the ability to make transactions 'anytime, anywhere'. However, at the same time, only 20 per cent of those surveyed agreed that making payments with mobile phones is secure while 40 per cent stated they would only use their mobile phones for small transactions such as buying coffee or a movie ticket. Only one

[179] See Legislative Council Press Release, website :< http://www.info.gov.hk/gia/general/200705/09/P200705090167.htm>. [Visited 22/6/2013].
[180] See Security Asia, (29 Aug. 2011) 'HK netizens' security awareness revealed' website: <http://security.networksasia.net/content/hk-netizens-security-awareness-revealed> [Visited 22/6/2013].

in eight were willing to use their mobile phones for purchases over HK$500. As Kerry Wong, General Manager of PayPal Hong Kong and Taiwan has said:

> "*Although many Hong Kong people appreciate the convenience of online payments, they are still hesitant to share their personal information online. People are reluctant to increase their use of online payment methods mainly because they don't know how to protect themselves and their private information online.*"[181]

Legislative Councilor for Information Technology sector, Charles Mok added that:

> "*Research by PayPal and City U reveals an apparent disconnect between Hong Kong people's high interest in using online and mobile payment methods with their low awareness and readiness to protect themselves against the potential risks,*"[182]

As a result of the popularity of online payment services and the regulatory requirements imposed by the HKMA, banks in Hong Kong were among the first in the world to implement two-factor authentication for their online banking customers.[183] This two-factor approach verifies the user's identity using 1) elements the customer knows (i.e. a password and user ID) and 2) elements the customer has in their possession (i.e. a digital certificate, security token or mobile-phone number).[184] Hence, banks in Hong Kong use relatively advanced technology to prevent Internet fraud. Accordingly, if a bank does detect a case of fraud, it should be able to produce and establish the electronic evidence required for criminal prosecution.

---

[181] Ibid.
[182] Ibid.
[183] See (July 2005) 'Banks move towards two-factor authentication'. Computer Fraud & Security. Volume 2005, Issue 7, p. 20.
[184] See the Hong Kong Association of Banks, (March 2007) Internet Banking Convenient & Safe Pamphlet.

Customer Contracts

Because banks are commercial entities they may consider it to be more cost effective to accept some liability for fraud and partially compensate the fraud victims, while at the same time limiting the terms and conditions governing the proper use of their online banking services. For example, condition 12.6 of the terms and conditions of the Bank of China's Internet banking service,[185] clause 12.1:

> *"Unless caused by our wilful misconduct or negligence, we are not liable for:*
> *a .any delay or interruption in your having access to an account or service, or any inability to use an account or service;*
> *b. any loss, error, delay, misdirection, corruption or unauthorised alteration or interception of a message sent through the internet, telephone or any other means, or any unauthorised access to a service, account or information;*
> *c. any act or omission including any failure to execute or error in executing your instruction;*
> *d. any error, malfunctioning, interruption, suspension or failure of any software, equipment or system;*
> *e. anything including any computer virus which may impair the functions of a computer system; or*
> *f. any loss or damage arising from termination of your account or any service provided to you."*

Condition 12.6 stipulates that the customers interpret and/or use the bank's website at their own risk. It reads:

> *"We have no duty to verify the validity or genuineness of any documents or the title to your property to be received or held by us."*

Condition 2.5 further states that the customers must not breach conditions 2.3 and 2.4, which require the customers to do all that they reasonably can to ensure the

[185] The Bank of China (Hong Kong). [Online] [Cited 11/11/2007]. Available from: <https://its.bochk.com/information/terms/ibs_tnc_main_e.html>.

secrecy and the security of their passwords at all times and to notify the bank immediately via a designated telephone number if the password has been compromised. It states:

> *"You will be liable for all losses if you have acted fraudulently or with gross negligence, allowed any third party to use your password or failed to comply with your obligations under Condition 2.3 or 2.4."*

The Bank of East Asia's (BEA) terms and conditions[186] for Internet banking are more specific, stating that the bank will only accept the loss to customers from any breach of security. According to Condition 9 provides:

> *"The customer understands and agrees that the failure on the part of the Customer to comply with any one of the following precautionary measures may lead to security breach and the Bank shall not in any event be held liable for any loss or damage whatsoever suffered by the Customer as a consequence thereof and the Customer shall:*
> *(a) At all times keep the Cyberbanking Account Number, the private key of Digital Certificate and/or password of Digital Certificate confidential, do not disclose the PIN and/or password of Digital Certificate to any person including any joint account holder of the customer; in particular, not to send them via electronic mail; and never assign the same PIN and/or password for accessing other services (for example, for connection to the Internet or accessing other websites);*
> *(b) notify the Bank immediately of any actual or possible unauthorised use of Cyberbanking Account Number, the PIN and/or Digital Certificate and shall confirm the same in writing without delay to the Bank;*
> *(c) not furnish the PIN and/or the password of Digital Certificate to anyone in any circumstances who claims to represent the Bank or holds out as the Bank's employee or authorised person (it is not necessary for the Bank's employee to know the PIN and/or the password of Digital Certificate);*
> *(d) logout the service and clear the browser cache after a banking session;*

[186] The Bank of East Asia. [Online] [Cited 11/11/2007]. Available from: <https://www.hkbea-cyberbanking.com/servlet/FR01Show?Lang=Eng&Channel=INTERNET>.

*(e) not leave the computer unattended while using Cyberbanking;*
*(f) not use public PC to access Cyberbanking;*
*(g) take caution of hackers and virus infection when sending and receiving emails, visiting and disclosing personal / financial information to unknown websites and downloading files or programs from websites;*
*(h) install proper firewall and anti-virus software and update them with security patches or newer versions on a regular basis to strengthen the security of the PC used by the Customer;*
*(i) upgrade browsers and application software to support SSL 128-bits encryption standard; and not select the option on browsers for storing or retaining users name and PIN and/or the password of Digital Certificate;*
*(j) remove file and printer sharing in PCs, especially when the customer has Internet access via cable modern, broadband connection, wireless or similar setup;*
*(k) change the PIN immediately by selecting a new PIN on the first usage and destroy those documents printed with the PIN subsequently;*
*(i) ensure not to use the Customer's identity card number, telephone number, date of birth, driving license number or popular number sequence (such as 987654 or 123456) when closing the PIN and/or the password of Digital Certificate; and not use the same digit more than twice;*
*(m) not write the PIN and/or password or Digital Certificate down, and shall memorise the same;*
*(n) keep the PIN and/or password of Digital Certificate separate from the Account Number and the Digital Certificate respectively;*
*(o) be alert to the surroundings before performing any banking transactions, and make sure that no one sees the PIN and/or password of Digital Certificate;*
*(p) for security reason, change the PIN and/or password of Digital Certificate regularly;*
*(q) check the authenticity of the Bank's website by comparing the URL and the Bank's name in its Digital Certificate and a security icon that like a lock or key appear when authentication and encryption is expected;*
*(r) notify the Bank of any change to the information provided to CA as soon as such change occurs and the Bank shall not in any event connection with the customer's failure to do so;*
*(s) not sure the Digital Certificate after it has been cancelled or revoked or has otherwise become invalid;*
*(t) set the password to protect the Digital Certificate immediately when receiving the Digital Certificate."*

Condition 9, the customer has to prove they have followed certain steps to prove they are not at fault.

BEA is so confident of the security of its computer system, condition 12 (a) specifically offers to compensate the customer if any loss resulting from computer crime is due to the failure of the bank's computer system. It states:

> *"Subject to the provision hereof and in the absence of negligence or default on the part of the Customer and the Customer has acted in good faith and with due diligence and also fully complied with the obligations under all the terms and conditions contained herein, the Customer shall not be liable for unauthorised transactions performed and/or executed through the Cyberbanking due to:*
> *(a) A computer crime not prevented by the security system of the bank; …."*

In contrast to the Bank of China's broad definition of the distribution of liability in its Internet banking terms and conditions, the BEA clearly defines and specific terms of the distribution of liability in the event of a breach of the security of its banking website. These examples show that the customers of the BEA are given a clearer understanding of what to do to protect their Internet banking accounts. The bank's terms and conditions also stipulate what the bank will do in the case of fraudulent transactions. Although the Bank of China and the BEA both accept liability, the BEA is much clearer and specific about under what conditions it will do so. Therefore, a customer who reports a fraudulent transaction to the Bank of China will probably find it more difficult to get compensation because the bank's terms and conditions are less specific and therefore more prone to interpretation. Alternatively, a customer of the BEA is likely to be asked a list of very specific questions, which will trigger a series of internal checks of the customer's

account. If the customer provides satisfactory answers to these questions, the bank will accept the complaint. The abovementioned terms and conditions suggest that the different banks in Hong Kong have different internal controls for Internet banking and that the banks use their terms and conditions to make it difficult for the consumer to verify their claims. However, the HKMA requires all banks to maintain a minimum standard of security.

Examples of Automated Teller Machine (ATM) Fraud

In 1982, ATMs were introduced in Hong Kong to offer customers the convenience of withdrawing their money at any time of the day or night. Today, the vast majority of consumers use ATMs and there are estimated to be at least 19 million ATM cards in circulation in Hong Kong[187] out of a population of approximately 7.3 million. In 1982, the Bank of China, the BEA, Chekiang First Bank, Shanghai Commercial Bank and Wing Lung Bank established a consortium called Joint Electronic Teller Services Ltd.[188] (JETCO) to provide a network of ATMs in Hong Kong. At the same time, two of the biggest banks, HSBC and Hang Seng Bank, developed a separate system known as the Electronic Teller Card (ETC). JETCO is currently the biggest ATM service provider in Hong Kong with network of nearly 1600 ATMs.[189] Customers can access their accounts through JETCO ATMs in Hong Kong, Macau and a few cities in mainland China. In recent years, ETC cardholders have been able to use their cards in similar places.

[187] The Legislative Council Debate, (24 March 2004) Hansard, p. 4882.
[188] See JETCO. [Online] [Cited 18/11/2007]. Available from: < http://www.jetco-online.com/compro.html>.
[189] Ibid.

Since November 2004, the payment card industry (including ATM operators) has been regulated under the Clearing and Settlement Systems Ordinance. The overall aim of the ordinance is to promote the general safety and efficiency of the clearing and settlement system[190] and the ordinance also designates the HKMA as its overseer. Although the HKMA encourages the payment card industry to adopt a self-regulatory approach, where the industry operators draw up a code of practice and monitor their own compliance, as the regulator, the HKMA monitors the overall implementation of the industry's self-regulatory measures under the requirements stipulated in the ordinance. The banking industry's own Code of Practice includes a number of requirements, one of which is incident reporting. Rule 16.1[191] states:

> *"Each payment card scheme operator should ensure a timely and efficient flow of relevant information to the HKMA of any incident (such as data security breaches) that it reasonably considers may have a material and adverse impact on its cardholders in Hong Kong or on the safety and efficiency of its payment card operations in Hong Kong."*

In addition, Rule 7.3[192] states that, on the technology system security:

> *"Each payment card scheme operator should conduct periodic security reviews of its system. Such reviews could be performed either by the payment card scheme operator or, at its discretion, by independent party appointed by it."*

And on supervision, Rule 14.1[193] reads:

---

[190] See Ibid [Cited 18/11/2007]. Available from: < http://www.jetco-online.com/pic/Code%20of%20Practice%20of%20Payment%20Card%20Scheme%20Operator%20(Eng)(final).pdf>.
[191] See Code of Practice Ibid [Cited 18/11/2007]. Available from: < http://www.jetco-online.com/pic/Code%20of%20Practice%20of%20Payment%20Card%20Scheme%20Operator%20(Eng)(final).pdf>.
[192] Ibid.
[193] Ibid.

> *"Merchant acquirers and card issuers of the payment card scheme operators that are authorised institutions in Hong Kong are subject to the licensing requirements under the Banking Ordinance and hence the prudential supervision by the HKMA."*

Under the above rules, the HKMA requests all ATM operators to audit their technology system security regularly (as shown rule 7.3 above). As the Secretary for Financial Services and the Treasury, Frederick Ma confirmed in the Legislative Council[194]:

> *"The banks' senior management is required to appoint an independent expert to commission an independent assessment of security [including technologies] aspect before the launch of the service, and generally thereafter at least once a year. The independent assessment report should be submitted to the HKMA."*

The above are important crime prevention measures. These measures are designed to stop fraud happening at an early stage by requiring the regular auditing of system security and the introduction of measures to detect if any crimes get through a bank's internal controls. Government regulations also stipulate that ATM systems have to be audited by an independent auditor. As a result, as we can see from the above quote, the Secretary for Financial Services and the Treasury has also indicated that the authorities prefer the ATM systems to be audited by independent auditors. Under such conditions, the victims of computer crime may have a better chance of accessing the ATM computer data, as this data can be provided by an independent auditor. Moreover, an independent auditor can provide a statement as to whether a bank's system is secure enough to have prevented the crime. If the answer is no, then it will be easier for the victim

[194] The Legislative Council Written Reply on 18 June 2003 to Hon. Sin Chung Kai questions [Online]. [Cited 18/11/2007]. Available from: <http://www.info.gov.hk/gia/general/200306/18/0618185.htm>.

to convince the bank that they are not at fault and to seek compensation for the loss incurred.

Furthermore, although banks and card-issuing institutions are not obliged by law to report the fraudulent use of their payment cards (including ATM cards) to the police,[195] rule 16.1 clearly specifies that if a crime is detected, the ATM operator must report the crime to the HKMA as soon as possible. The HKMA will then alert the police, who will investigate and prosecute the fraud. This may lead to the fraud entering the criminal justice system. Furthermore, as almost all ATM operators are banks, they are subject to the much more stringent supervision imposed by the Banking Ordinance (rules 14.1 above), as well as the payment card industry Code of Practice. Therefore, the interests of ATM users in Hong Kong are well protected.

Although the banks have no statutory duty to report instances of ATM fraud directly to the police, the fact they have to report such crimes to the HKMA means that the fraud will eventually come to the attention of the police. Therefore, although seemingly self-regulated, Hong Kong banks are in fact heavily regulated by the HKMA. Because banks are also required by law to strictly follow the Code of Banking Practice, they are also in effect subject to external regulation, because failure to do so would result in loss of their licences. In theory, all Internet banking fraud (including ATM fraud) should come to the attention of the authorities. However, it is difficult to know if this is true, as the

[195] Legislative Council Debate, (24 March 2004) Op Cit.: p. 4863.

Hong Kong authorities do not generally maintain a regular record of cases of ATM fraud.

At one point, in the early 2000s, Hong Kong experienced a sudden surge in reported cases of ATM fraud, as shown in Table 4.5 below.

**Table 4.5: Cases of ATM Card Fraud Committed in Hong Kong with Stolen or Lost Cards**

| Year | 11 Oct 2002 - 19 Nov 2003[196] | 2004 | 2005 | 2006 | 2007 (Jan-Jun) |
|---|---|---|---|---|---|
| **Nos. of reported Cases** | 50 | 1043 | 801 | 644 | 330 |
| **Reported amount of losses (Million in HK Dollar)** | 2.1 | 21.65 | 17.04 | 20.77 | 7.02 |

*(Source: Legislative Council Question 16)* [197]

This sudden rise produced questions in the Legislative Committee, as the figures provided the first indication of the extent of ATM fraud in Hong Kong. The numbers jumped from 50 cases amounting to HK$2.1 million in 2003 to 1043 cases and total loss of HK$21.65 million a year later. In subsequent years the numbers began to drop, with the figures for 2005, 2006 and the first six months of 2007 corresponding to 801, 644 and 330 cases, respectively. The authorities[198] claimed that the drop in ATM fraud was the result of measures implemented by the banks to prevent ATM fraud, such as limiting the amount of cash that could be withdrawn within from an ATM during a 24-hour period. The Consumer

[196] The Consumer Council. [Online] [Cited 18/11/2007]. Available from: <http://www.consumer.org.hk/website/ws_en/news/press_releases/p32803.print>.
[197] See Legislative Council, 'Prevent Payment Card Fraud Cases' (Written Answer, on 14 November 2007). [Online] [Cited 18/11/2007]. Available from: <http://www.info.gov.hk/gia/general/200711/14/P200711140227_print.htm>.
[198] Legislative Council, question raised by Hon. David Chu on curbing ATM-related theft cases, written reply by the Secretary for Security, Ambrose S.K. Lee, see LCQ8: Curbing ATM-related theft cases, (14 January 2004). [Online] [Cited 18/11/2007]. Available from: <http://www.info.gov.hk/gia/general/200401/14/0114145.htm>.

Council reported[199] that the banks had also introduced measures to continuously monitor ATMs, such as closed-circuit television (82 per cent) and anti-spy-camera devices (18 per cent[200]). Other measures that the Consumer Council reported include: 1) installing a mechanism that records the relevant information on ATM cards and credit cards so that a bank can determine whether an unauthorised ATM transaction has been carried out using a counterfeit card (implemented by 57 per cent of the banks); 2) increasing the frequency of the patrols of ATMs during and after opening hours by private security guards or the police (88 per cent); 3) encouraging customers to report any suspicious devices (skimming devices) detected on ATMs and providing a hotline telephone number (88 per cent ); 4) proactively alerting customers if any unusual transactions appear in their accounts (75 per cent) and 5) installing anti card-skimming devices on ATMs. [201]

In addition to these preventive measures, the police in Hong Kong actively investigate and prosecute reported cases of fraudulent card use and maintain a close liaison and intelligence exchanges with banks and the credit card industry.[202] The Hong Kong Association of Banks, the police and the HKMA have also closely co-operated in producing a number of initiatives to educate

[199] The Choice, (February 16, 2004) 'New arsenal of security measures to fight ATM fraud unveiled', The Consumer Council, No. 328. [Online] [Cited Viewed 18/11/07]. Available from: <http://www.consumer.org.hk/website/ws_en/news/press_releases/p32803.print>.
[200] Ibid.
[201] Ibid.
[202] For example, on 17 November 2007, the MingPao Daily (Chinese) newspaper reported that a man was prosecuted by the Commercial Crime Bureau (CCB) of the Hong Kong Police and convicted at the Kowloon City Magistrates' Courts for using a fake ATM card.

consumers in taking precautions against fraud[203] (e.g. local radio and TV programmes).

Despite these preventive measures, ATM fraud still happens. The question remains then as to what the banks can do when fraud occurs. In Hong Kong, the ATM cardholder is not liable for any losses if the transaction was not authorised by the cardholder or the cardholder did not act fraudulently.[204] As the Code of Banking Practice, Rule 29.1 reads:

> *"Liability for loss*
> *Card issuers will bear the full loss incurred-*
> *(a) in the event of misuse when the card has not been received by the cardholder;*
> *(b) for all transactions not authorized by the cardholder after card issuer has been given adequate notification that the card/PIN has been lost or stolen or when someone else knows the PIN (subject to paragraph 29.4 below);*
> *(c) when faults have occurred in the terminals, or other system used, which cause cardholders to suffer direct loss unless the fault was obvious or advised by a message or notice on display; and*
> *(d) when transactions are made through the use of counterfeit cards."*

However, to qualify for an exemption of loss, the ATM cardholder still has to have followed all the terms and conditions of the contract. For example, Wing Hang Bank's contract (Section 8- Lost Card Liability) states as follows:

> *"8.1 In case of any loss, theft or misuse of the Card or Card Account Number or PIN, the Cardholder must upon discovery immediately report such loss or theft or misuse to the Bank's Card Centre and confirm the loss or theft or misuse in writing thereafter. The Cardholder undertakes to give the bank and police all the information*

[203] Legislative Council Question Debate, (18 June, 2003). [Online] [Cited 18/11/2007]. Available from: <http://www.info.gov.hk/gia/general/200306/18/0618185.htm>.
[204] The Code of Banking Practice, Rules 29.4. [Online] [Cited 19/11/2007]. Available from: <http://www.info.gov.hk/hkma/eng/bank/e-banking/cobp.htm>.

> *in the Cardholder's possession as to the circumstance of any loss or theft or misuse of a Card and to take all reasonable steps to assist the bank to recover the lost card.*
> *8.2 The cardholder shall be liable for all amount debited to the Card Account as a result of the unauthorised use of a Card Account Number or PIN until notification of its loss, theft or disclosure has been received by the Bank. The Cardholder will not be liable to the amounts debited to the Card Account, which arise from the unauthorised use of the Card where the Cardholder has not acted fraudulently, with gross negligence in safeguarding the Card or Card Account Number or PIN and has not failed to inform the Bank as soon as reasonably practicable after having found that his or her Card or Card Account Number or PIN has been lost, stolen or disclosed to a third party.*
> *8.3 Unless the Cardholder has acted honestly, in good faith, with due care and notification to the Bank, and has followed any measures to safeguard the Card, PIN and such Card Account Number as recommended by the Bank in its communication to the Cardholder from time to time, the Cardholder shall be liable for all amount, without limit, debited to the Card Account."*

Nonetheless, customers in Hong Kong have better prospects of being compensated for ATM fraud losses. For example, the Consumer Council[205] reports that of 50 cases of suspected ATM fraud between 11 October 2002 and 19 November 2003, 49 cases were settled and compensated with victim receiving the full amount of the loss from the bank. The banks reimbursed around HK$2.1 million in total to the account holders, with the highest amount being HK$377,000 and the lowest HK$1,900. In Hong Kong, the burden of proof does not rest with the consumer. Rather, the banks have to prove that their computer systems are not at fault. Moreover, even if a bank has compensated a victim and they have resolved the matter, the bank must still report the fraud to the authorities, and the HKMA will subsequently alert the police. The police may not

[205] The Choice, (February 16, 2004) Ibid.

investigate the case if it has been resolved. Therefore, evidence of the fraud may not enter into the criminal justice system.

In the next section, I examine whether the consumer faces the same protection when engaging in Internet banking.

Internet banking

In Hong Kong, there is no consensus on the distribution of liability for Internet banking fraud. In February 2007, the Hong Kong Consumer Council (HKCC) surveyed 20 online banks,[206] of which 17 banks responded. The survey inquired about the compensation for loss if things go wrong while customers are banking online. The banks answered that unless customers can prove that their losses are a result of a bank's gross negligence or wilful default, they are unlikely to be compensated. The survey also asked about compensation for loss in the event of an Internet banking system breakdown. In this case, 9 out of the 17 banks (53 per cent) stated they would adopt a 'case-by-case' approach, but they would not commit themselves to paying out compensation to affected customers. The remaining 8 banks (47 per cent) expressly declined any liability for monetary loss. The survey also inquired about compensation for consumers who had logged into 'fake' websites. In this case, 9 banks (53 per cent) stated they would consider redress on a 'case-by-case' basis, while 5 (29 per cent) would assume liability only if the loss was caused by their own gross negligence. The remaining 3 banks (18 per cent) declined any liability for such losses.

[206] The Hong Kong Consumer Council (February, 2007). The Choice No. 364 (Chinese). [Online] [Cited 27/02/2007]. Available from: <http://www.consumer.org.hk/website/ws_en/news/press_releases/p36401.html>, p. 32.

Notably, many of the banks' survey responses contradict Clause 40 of the Code of Banking Practice, which states that unless customers act fraudulently or with gross negligence, they should not be responsible for any direct loss suffered as a result of unauthorized transactions conducted through their accounts. Although on paper customers in Hong Kong seem to be well placed, in practice, banks often try to wriggle-out of their statutory responsibilities. However, if a complaint is referred to the HKMA, HKAB or HKCC, then the bank will be forced to reassess the situation.

While the HKMA considers the issue of compensation as a matter between the banks and the customers, the banks are required to follow guidelines on complaint handling procedures and the Code of Banking Practice by setting up an internal complaint mechanism to ensure that customer complaints are dealt with swiftly and justly. As the HKCC[207] has stated, according to the HKMA's experiences, when consumers produce proof that their loss is caused by a bank's Internet system failure, the cases are resolved satisfactorily by the banks. This shows that the banks' internal complaint handling systems are working.

In Hong Kong, customers generally have to prove that they have not acted negligently. However, they do not need to produce proof that the bank's computer system is the problem, as the Code of Banking Practice specifies that unless the bank can prove that the customer has acted fraudulently, the customer should not be responsible and should be compensated for any losses they incur. In this case, it is up to the bank to show that its computer system is not at fault.

[207] Ibid.

Whistle-blowing

In theory, Internet banking fraud in Hong Kong can be exposed through whistle-blowing.[208] However, Hong Kong has not enacted a 'whistle-blower's act' or the equivalent for any person who raises concerns about their employer's misconduct or illegal actions. Even those who make an official corruption complaint to the Independent Commission Against Corruption (ICAC) do not have whistle-blower protection, although the ICAC will treat the complainant's identity as strictly confidential. There have been a number of occasions where there has been public debate as to whether Hong Kong should have its own whistle-blowing legislation. For example, in 1999, during consultation for legislation on the civil liability for the invasion of privacy, the Hong Kong Law Reform Commission and its sub-committee on privacy briefly considered whether some protection should be given to whistle-blowers in cases where it is in the public interest to disclose private information. However, the Commission rejected the proposal.[209] In 2003, during Legislative Council debate on the controversial National Security Bill,[210] there were numerous calls for whistle-blower protection to be added to the bill. However, the government refused to add such a measure.[211]

[208] According to the PriceWaterHouseCoopers Global Economic Crime Survey 2005, 34 per cent of the fraud detected in organisations located in Hong Kong were through either internal or external tip-offs. See PriceWaterHouseCooper. [Online] [Cited 19/11/2007]. Available from: <www.pwc.com/crimessurvey>.

[209] See the Law Reform Commission of Hong Kong, (1999) Sub-Committee on Privacy, Consultation on Civil Liability for Invasion of Privacy, HKSAR., para. 11.120, p. 160.

[210] Under Article 23 of the Basic Law of the HKSAR, as part of China, the HKSAR government has a constitutional duty to enact the national security laws.

[211] See the HKSAR government, Basic Law 23. [Online] [Cited 18/05/07]. Available from <http://www.basiclaw23.gov.hk/english/resources/legco/legco_article/article17.htm>. However, after a mass street protest in early July 2003, the government eventually withdrew the enactment of the National Security Legislation Provisions Bill on 5 September 2003.

People in Hong King rarely make complaints via the whistle-blowing process. As Chiu[212] states, ethics are culturally specific. For instance, what is considered ethical in Western society may be unethical in another society. Ahmed et al.[213] also observe that cultural differences influence the perception and awareness of the ethical consequences of business practices. Whistle-blowers in many Western societies can be regarded as model employees. However, as Chiu[214] points out, in Chinese society, whistle-blowing is considered unacceptable and unethical behaviour by many model Chinese employees, because it breaks the close tie between the employee and the employer. Moreover, loyalty and trust are seen as the cornerstones of the employment relationship in Chinese society. As Lam[215] states, classical Confucian doctrines also have a direct bearing on business, the development of trust and the observation of proper rites or *li* (etiquette), including sincerity as emphasised in the doctrine of the mean. Chiu also argues[216] that Confucian virtue urges social conformity and harmony. As this tradition helps shape labour relations in Hong Kong, it could have a number of ramifications for someone who blows the whistle. For instance, a whistle-blower could lose their employment, which may also mean that he or she lose his or her company subsidies, such as housing and health benefits, as well as incurring threats of revenge from family members and colleagues. A whistle-blower may also be considered a disloyal member of the organisation and be socially isolated at work

[212] Chiu, R.K. (March I-II 2003) 'Ethical Judgement and Whistleblowing Intention: Examining the Moderating Role of Locus of Control', Journal of Business Ethics, Vol. 43, Nos. 1-2, p. 66.
[213] Ahmed, M.M., Kung, Y.C. and Eichemseher, J.W. (March I-II 2003) 'Business Students' Perception of Ethics and Moral Judgement A Cross-Culture Study', Ibid, p. 100.
[214] Chiu, R.K. (March I-II 2003) Ibid.
[215] Lam, K.C.J. (March I-II 2003) 'Confucian Business Ethics and the Economy', Ibid, pp. 154-155.
[216] Chiu, R.K. (March I-II 2003) Ibid.

by both peers and management. As Snell and Herndon[217] state, in Hong Kong, manager-subordinate relations appear to follow a ruler-subject pattern, where subordinates are expected to follow their master's will and doing otherwise would be regarded as disloyal and improper.

Because of the abovementioned cultural factors, whistle-blowing is unlikely to be wide-spread in Hong Kong. Simply put, potential whistle-blowers will be reluctant to come forward, because they will not be protected by law, and their whistle-blowing could have serious financial consequences for the individuals and their families. In addition, there is no comprehensive social security system available in Hong Kong for anyone who is sacked from their employment. In some cases, an organisation may even pursue a whistle-blower in court for damages for disclosing the company's confidential information. As the first of the case samples (**Case 1)** confirms, whistle-blowers can face prosecution in Hong Kong.

Internal Bank Audits

A case of fraud may be detected during a bank's routine internal audit. In Hong Kong, the principles of audit reporting are similar to those in many places around the globe, including the UK. As Lam and Mensah[218] state, Hong Kong adopted the UK auditing standards prior to the transfer of sovereignty on July 31, 1997. According to the Hong Kong standards, auditors must be approved by the HKMA

[217] Snell, R.S. and Herndon, Jr. N.C. (April (II) 2004) 'Hong Kong's Code of Ethics Initiative: Some Differences between Theory and Practice', Journal of Business Ethics, Vol. 51 No.1, pp. 76-77.
[218] Lam, K.C.K. and Mensah, Y.M. (2006) 'Auditors' decision-making under going-concern uncertainties in low litigation-risk environments: Evidence from Hong Kong', Journal of Accounting and Public Policy, Vol. 25, p. 711.

before they are allowed to conduct any auditing work in a bank. Auditors are also statutorily required under the Banking Ordinance to report any crime discovered during an audit. In 2003, the Secretary for Financial Services and the Treasury, Frederick Ma,[219] reported the figures on reported banking fraud to the Legislative Council in response to a question about the efficiency of the auditor reporting system. The number of Internet fraud cases reported to the HKMA by auditors appears to vary year to year. For example, there were 171 reported cases in 2001, but only 40 in 2002. However, none of these cases involved penetrating a bank's computer security systems.

As in the UK, a bank auditor in Hong Kong is employed by the bank's board of directors and reports to the board. The main aim of an Internet banking audit is to review the bank's operating procedures to ensure the bank has complied with its regulatory requirements. This involves: (a) checking whether the bank's online banking system incorporates adequate internal controls and complies with the policies approved by the organisation or the supervisory authority (such as the relevant codes of practice and laws), (b) reviewing all operations to confirm that the essential Internet firewall and anti-virus systems are up-to-date), and (c) testing whether the banks internal controls are sufficient to minimise error and discourage fraud. Importantly, an audit also ensures that a bank's computer system records all electronic transactions and that the records provide a clear audit trail. If a particular problem is discovered during an audit, the auditor is expected to assist management in developing an appropriate solution. In particular, the audit tests whether management have instituted the appropriate

[219] Legislative Council Question Debate, (18 June, 2003) Ibid.

controls to deal with the type and level of risk arising from online banking in Hong Kong (e.g. they are sufficiently fast and accurate to enable customers to trade in stocks and shares online).

Although Hong Kong's audit reporting principles are similar to those in the UK, the different legislative and regulatory requirements in different jurisdictions mean that auditing standards can still vary from country to country. For example, section 240 of the Hong Kong Standard on Auditing[220] was revised in 2004 to incorporate section 61 of the Banking Ordinance.[221] This gave auditors the option of reporting fraud directly to the HKMA, providing they make the complaint in 'good faith'. The revised standard also provides protection for the complainant in case they get sued for disclosing the bank's confidential information. The commercial objective of hiring auditors is to create the impression that banks' online systems are transparent and that the banks have systems in place to identify any attempts to commit online fraud. If an auditor detects a case of fraud, they will usually notify the bank and report the incident to the HKMA. If the fraud is reported to the bank then the bank can decide whether to report the matter to the police. In theory, the chances of this are high because the Code of Banking Practice stipulates that banks ***must*** report any instances of crime to the authorities. Even if the bank simply closes the loophole (with or without compensating the victim), it is still supposed to report the fraud to the authorities.

[220] See Hong Kong Institute of Certified Public Accountants, (October 2004) Hong Kong Standard on Auditing: The Auditor's Responsibilities to Consider Fraud in an Audit of Financial Statements, Hand Book Section 240.
[221] See Hong Kong Monetary Authority Guideline No. 9.1 Banking Ordinance: Section 61 (reporting by auditors under section 61). [Online] [Cited 14/11/2007]. Available from: <http://www.info.gov.hk/hkma/eng/guide/guide_no/guide_91b.htm>.

Because auditors have a legal duty to report any instances of crime to the authorities, all cases of Internet banking fraud should enter the criminal justice system. However, if an auditor is hired by a bank, the auditor is faced with a potential conflict of interest in that they have a legal duty to report crime to the authorities and are at the same time expected to be loyal to the bank employing them. If an auditor discovers a borderline case of fraud, he or she may treat it as a minor book entry error and correct it themselves, instead of reporting the matter to senior management. If this happens, then the Internet fraud will not be reported to the bank and is unlikely to ever enter the criminal justice system. According to an empirical study by Leung,[222] in the early 1990s, most Hong Kong auditors did not have a background in computer education, even though they were expected to prevent and detect computer fraud. In fact, at this time, the auditors felt that the responsibility for preventing and detecting computer fraud rested with management. However, the HKMA also regulates the auditors and if an auditor is found to have failed to report a crime to the authorities, they are likely to be de-listed from the list of approved auditors. However, it is not clear how the failure to report an incident would come to light.

In theory, Hong Kong's internal audit system should provide rigorous reporting controls and accurate statistics on Internet banking fraud. However, in practice, as in other countries, the auditing system is oriented more towards satisfying the interest of the banks than to detecting and reporting fraud to the police. Although the supervisory regulations in Hong Kong require banks to report any instances

[222] See Lee Tse-Leung, R. (1996) A Descriptive Study of Audit Practice in Hong Kong in Relation to Computer Fraud. MA. Thesis (Unpublished). The City University of Hong Kong.

of crime to the police, but as we shall see the interview data in this thesis suggest that this is not always the case.

The Victim Reports Fraud Directly to the Bank

In some instances, the customer will report a case of fraud directly to the bank. In this case, if things go wrong between the bank and the consumer, the only protection for the customer other than the relevant consumer protection laws is the terms and conditions written in the contract. Here, the consumer's rights and liabilities are specified in the 'small print' in the contract between the consumer and the bank. Nonetheless, the banks have to follow the Hong Kong Code of Banking Practice. Although adherence to the Code is voluntary, the HKMA expects all banks and financial institutions to join when they apply for their banking licence. Moreover, if a bank does not follow the Code, it may lose its banking licence.

In recent years, the HKMA has strengthened the level of consumer protection for Internet banking and introduced a statutory complaints procedure for all banks. The statutory procedure requires banks to immediately close or freeze compromised Internet bank accounts when their complaint handling departments receive consumer complaints. The information technology system administrator is then expected to plug the loophole in the Internet server that enabled the fraud to occur to stop further funds being withdrawn from the account. To comply with the Code of Banking Practice, the bank must reply to the account-holder and acknowledge the complaint within 7 working days. The bank must inform the account-holder that the compromised Internet account has been closed for

investigation and the bank is dealing with the problem. At the same time, the bank is required to conduct an initial fraud investigation either in-house or private investigator. The bank must then communicate its decision about the case to the complainant within 30 working days. Depending on the nature of the complaint, the bank must provide a final written response to the complainant no later than 60 working days after receiving the complaint.[223] Here, the bank has two main options in that it can write to the complainant to either inform them that the bank has reached a final decision or specify clearly what has been done thus far, but requesting more time to resolve the complaint.

If a bank takes the first option, there are a number of different ways in which it can resolve a complaint. For example, the bank may:

(1) Accept the loss and decide to fully compensate the victim fully to retain a good business relationship with the client. This would be the end of the matter. However, the bank will also report the matter to the HKMA and the police. However, the bank may only accept some liability and pay partial compensation to the victim.

(2) Inform the customer that it has rejected the complaint and fully explain the reasons for doing so. The bank must also explain to the customer that if they are not satisfied with the decision, they can take the complaint further, by referring it to the HKMA or the Hong Kong Association of Banks.

(3) Inform the customer that it has reported the complaint to the police, and allow the police to take over the matter as a criminal investigation. The bank may ask

[223] See Hong Kong Monetary Authority, Complaint Handling Procedure Policy Manual, IC-4, V.1-22.02.02. [Online] [Cited 07/03/2007]. Available from: <http://www.info.gov.hk/hkma/eng/bank/spma/attach/IC-4.pdf>, para. 3.2.2, p. 9.

the customer to co-operate with the police. In regard to compensation, the bank may inform the complainant that it will address the issue after the criminal investigation has been completed, although the matter will still be subject to the terms and conditions agreed upon in the Internet banking contract.

The HKMA complaint handling procedural manual[224] requires banks to retain their complaint records in a convenient and accessible form to facilitate either regular or ad-hoc inspections by the HKMA. The HKMA can request a bank to report the number and type of complaints it has received and the manner in which they have been resolved.[225] The HKMA has also specified that banks must provide details of a single contact for handling complaints within one month of receiving their banking licences and that they should update the HKMA if the contact changes.

The Bank Rejects the Complaint

A bank may reject a complaint after it has been thoroughly investigated in-house and clarify the reasons to the customer in accordance with the terms and conditions listed in the contract. However, what happens next depends on the bank's commercial approach to apportioning liability due to fraud, and which bank the customer has a relationship with. All banks must explain clearly to the customer how to take the complaint further, by referring it to the HKMA or HKAB.

[224] See Hong Kong Monetary Authority, Complaint Handling Procedure Policy Manual, IC-4, V.1-22.02.02, [Online] Op Cit.: para. 5.1.1-5.1.2, p. 10.
[225] See Hong Kong Monetary Authority, Complaint Handling Procedure Policy Manual, IC-4, V.1-22.02.02, [Online] Op Cit.: para. 4.2.1-4.2.2, p. 10.

Those within the bank with the authority to reject the complaint will decide either (1) that the case should be put down to experience or (2) that the bank should seek to recover its costs against the complainant through the civil courts. However, in the latter case, the banks will weigh the costs, such as the cost of hiring lawyers, before any action is taken. Civil litigation is a serious consideration in Hong Kong, because the extremely high legal costs in Hong Kong deter many from taking civil action.[226] This has fuelled complaints that the courts are only accessible to the rich. Again, if the victim disagrees with the result, he or she can refer the case to the HKMA or HKAB (there is no financial ombudsman in Hong Kong).

When the HKMA Reports a Case of Internet Fraud to the Police

Hong Kong banking regulations specify that banks haves to report any cases of Internet fraud to the HKMA. Although the HKMA does not carry out criminal investigations or prosecutions, it will normally pass the information on to the relevant agencies, such as the police or the ICAC.

The Hong Kong Monetary Authority (HKMA) was established under the 1992 Exchange Fund (Amendment) Ordinance[227] by merging the Office of the Exchange Fund with the Office of the Commissioner of Banking. As an integral part of the government, the HKMA is directly answerable to the Financial Secretary. The powers and responsibilities of the HKMA, which are similar to the

[226] Hensrude, G. (2002) 'Awakening Hong Kong's Sleeping Lion: A Case for Increased use of O 62 R8', Pacific Rim Law and Policy Journal, Vol. 11, No. 2, p. 373.
[227] See HKMA, (2004) Annual Report 2004, p. 9.

FSA, are set out in various ordinances,[228] such as the Exchange Fund Ordinance, the Banking Ordinance, the Deposit Protection Scheme Ordinance and the Clearing and Settlement System Ordinance. Under the Banking Ordinance, the HKMA is empowered to regulate the activities of banks, deposit-taking companies and non-deposit-taking financial institutions. According to the annual report of the HKMA, in supporting the Financial Secretary, the HKMA is responsible for various statutory objectives,[229] including a) promoting the general stability and effective working of the banking system, b) promoting the safety and efficiency of the financial infrastructure through the development of payment, clearing and settlement systems and, where appropriate, the operation of these systems, and c) promoting, in co-operation with other relevant bodies, confidence in Hong Kong's monetary and financial systems, and market development initiatives to help strengthen the international competitiveness of Hong Kong's financial services. The task of maintaining the safety and soundness of the Hong Kong banking system is shared among three departments: 1) the banking supervision department (which has five divisions handling the day-to-day supervision of banks); 2) the banking policy department (which has three divisions that formulate supervisory policies) and 3) the banking development department (which also has three divisions formulate policies and pursue initiatives to promote the development of the banking industry in Hong Kong).[230]

[228] HKMA, (2004) Op Cit.: p. 10.
[229] HKMA, (2004) Op Cit.:p. 11.
[230] HKMA, (2004) Ibid.

One of the respondents interviewed for this research was a senior Hong Kong banker who had previously worked in HKMA as a regulator overseeing the banking industry in Hong Kong. He described the course of action the HKMA would normally take when banks were found to have contravened the Banking Code and the Guidelines:

1. *"The HKMA would appoint an external auditor to audit the bank. If it is a very serious suspected case, the HKMA would employ a third party to audit the suspect bank and report back to the HKMA directly. If it was a less serious suspected case, then the HKMA would request the bank's own auditor to audit the bank itself and file a report to the HKMA as to what action to take;*
2. *After it has received the auditors' report, the HKMA would decide - if it is a less serious case - that the bank take corrective action. If it's a more serious case, internally the HKMA would send a team of auditors to interview the bank's senior management over a number of days. After the interview, if the bank shows no improvement or no corrective action is taken about the suspected wrong doing, then the matter would be referred to the HKMA Committee;*
3. *The HKMA Banking Stability Committee will consider the matter, then decide what course of action to take. There are basically three courses of action:-*
    - *i) Immediate disciplinary action:- a fine or a warning letter or both, attached with a restriction on the bank's commercial activities (ie. the bank is basically on the HKMA's watch list);*
    - *ii) Refer the matter to another authority to look into the matter for suspected corruption or fraud (ie. refer to ICAC and/or the police)*
    - *iii) If the bank is found guilty as charged in court, then the HKMA either takes away the bank's licence or merges it with another local bank in Hong Kong. Since the mid-1990s, merging with a local bank has been the most preferred route for the HKMA, because it would retain some degree of employment and the reputation of Hong Kong as a world leading financial centre; and it is a less destabilising shock to the financial market, therefore maintaining international investors' confidence in Hong Kong."*[231]

Theory Vs Practice

Thus far, this chapter has looked at the ways in which cases of Internet fraud and similar types of theft are dealt with via banks' internal control systems and these crimes subsequently come to the attention of the criminal justice system. As a

[231] E-mail Interview to a senior local banker and replied the researcher on 23rd April, 2009.

reflection of the understanding of the need for Internet security in Hong Kong, most banks have installed Internet security systems that go beyond the minimum requirements of the HKMA. These systems not only stop most Internet fraud from occurring at an early stage, they are also important for prosecution. If Internet fraud *does* happen, good Internet security may also help provide a vital source of electronic evidence, which will enable the police to establish proof when the bank reports the crime to the authorities. Nevertheless, some cases of Internet fraud will go undetected until the bank is alerted by other means, such as a report by the victim or (very rarely) whistle-blowing by one of its own employees.

The HKMA is a quasi-governmental institution that has the power to investigate Internet banking fraud and to require banks to report instances of fraud to itself and other authorities. The HKMA has the power to de-licence any bank that fails to follow the Banking Code or the banking guidelines. These powers should mean that the HKMA has enough 'teeth' to force the banks to report Internet fraud and to improve their banking security.

In theory, if a case of Internet banking fraud is detected through an HKMA audit, the authority is mandated to report the crime to the police. If the online banking fraud is detected through a bank's own audit, the bank must in theory report the crime to police. The bank can also report the incident to a number of other authorities, such as the FSC and the ICA. Along with the HKMA, these institutions play a key role in identifying and prosecuting foul play in the financial and banking systems.

However, the data indicate that theory and practice sometimes differ, and that the system of reporting may not be as efficient as the regulations suggest. As aforementioned, various government institutions, such as the HKMA (set up in 1993), police and ICAC, as well as non-government statutory bodies such as the Financial Reporting Council (set up in 2006), and the Securities and Futures Commission (set up in 1989) oversee the detection and reporting of Internet fraud in Hong Kong. The courts also play a part, as do a number of international bodies, such as the Bank for International Settlements[232] (BIS), which set up a representative office in Hong Kong in 1998 and Basel II.[233] These are all part of the external environment within which the identification and investigation of Internet fraud operates in Hong Kong. On paper, a bank will normally institute its internal decision making processes after it has received and acknowledged an alleged fraud complaint. Paragraph 4.5 of the HKMA's supervisory policy manual on the supervision of e-banking[234] states that banks should put in place formal incident response and management procedures for the timely reporting and handling of suspected or actual security breaches, acts of fraud or interruptions of their e-banking services during or outside office hours. According to the procedure manual, banks are allowed some time before they are required to respond to the complainant. They must use this time to determine the

[232] BIS originally established an office in 2000 to advise on things such as risk control in the banking sector.
[233] Basel II is the second of the Basel Accords. The purpose of the Accord is to improve banks' internal controls on risk management and capital supervision etc. More importantly, the Accord encourages banks to identify risks, including fraud, at the earliest possible stage. See Basel II. [Online] [Cited 31/10/2008]. Basel: Bank for International Settlements. Available from: <http://www.bis.org/publ/bcbs128.htm>.
[234] See Hong Kong Monetary Authority, Supervision of E-Banking, TM-E-1, V.1-17.02.04. [Online] [Cited 07/03/2007]. At <http://www.info.gov.hk/hkma/eng/bank/spma/attach/TM-E-1.pdf>, para. 4.5, p. 17.

origins of the incident (especially whether or not it is a result of the weakness of the bank's own security controls or operating environment). The bank should also the assess (i) the potential scale and impact of the incident, (ii) whether to report the matter to senior management and (iii) whether the incident is capable of damaging the bank's reputation or causing material financial loss. The bank should also strive to contain the damage to the bank's assets, data and reputation, and to the customer. Importantly, the bank should collect and preserve forensic evidence of the crime to facilitate any subsequent investigation or prosecution

The HKMA policy manual also outlines the conditions of liability between a bank and its client.[235] In providing e-banking services to their personal customers, the banks are required to observe the Code of Banking Practice. Accordingly, the banks must clearly state their terms and conditions, which should be fair and balanced to both the institutions and the customers. The HKMA holds that unless a customer acts fraudulently or with gross negligence, customers should not be considered responsible for any direct losses suffered as a result of unauthorized transactions conducted through their accounts. The bank may wait for the results of the initial fraud investigation, carried out in-house or by a private investigator, before they decide what to do next. There are a number of options available to the bank at this stage:

**a)** The bank can accept the complaint and compensate the victim fully for the loss. This will be the end of the matter. However, the HKMA's policy manual[236] states that banks **must** report such incidents to the authorities and retain the

[235] Ibid. para. 5.1.1-5.1.2, p. 20.
[236] See Hong Kong Monetary Authority Supervisory Policy Manual, IC-4, Complaint Handling Procedures, V.1-22.02.02. [Online] [Cited 11/03/2007]. At <http://www.info.gov.hk/hkma/eng/bank/spma/attach/IC-4.pdf>.

details of the complaint for at least two years from the date of receipt. The details include the complainant's name, the substance of the complaint and any communication between the bank and complainant, including how the complaint was resolved.[237] If a complaint is referred by the HKMA or another party,[238] the bank is expected to co-operate fully with the HKMA in handling the complaint against them. The HKMA expects bank to fully investigate complaints and to report them to the police. The bank concerned is expected to submit the findings from its investigation, together with copies of any correspondence with the complainant, to the HKMA as soon as possible. Normally, banks are expected to submit their findings no later than thirty days after the date of the initial letter from the HKMA.[239]

**b)** The bank can accept some liability and partially compensate the victim according to the terms and conditions of the bank's online banking service and report the matter to the authorities.

**c)** The bank can inform the customer it has rejected the complaint and fully explain to the customer the reasons for doing so in accordance with the terms and conditions listed in the online banking contract. The bank will then file a report with the HKMA to fulfil its obligations under the Code of Banking Practice. The HKMA **must** report the matter to the police. (However, the HKMA only reported Internet banking fraud to both the ICAC and the police in one of the 15 case studies, **Case 5,** presented in Chapter Nine of this thesis).

[237] The Hong Kong Monetary Authority. Op Cit.: para. 4.1, p. 9.
[238] Other parties include the Legislative Council, the Consumer Council, the District Council and the Media, see the Hong Kong Monetary Authority. Op Cit.: para. 5.3.1, p. 10, footnote 2.
[239] The Hong Kong Monetary Authority. Op Cit.: para. 5.2-5.3, p. 10.

**d)** The bank can inform the customer that it has decided to report the complaint to the police and the HKMA, and ask the customer to fully co-operate with the investigating authorities.

However, some banks do not report all such matters to the police, especially if they fall into a grey area or are border line cases. Instead, in these cases, the banks will normally try to find an alternative solution to resolve the matter with the customer. As an e-banker interviewed for this research said:

> "*I don't think I can cite any specific situation, but in general…the general mentality or the general culture in dealing with this kind of computer crime… is, because people here [inside the bank] are usually afraid to talk about it, they try to cover it rather than…because of the reputational issues.*"[240]

He explained:

> "*I think, there are two sides. From the business side or as the owner of the e-banking business, we want to have, as I said before, we want to have a better understanding or better awareness of this kind of computer crime…among the users… to protect the security of the system. But from the management side or from the general business side, they would think that if anything happened, they really want to cover it up, rather than exposing it. We are putting certain services or certain products to the customer, but if there is a situation happening [crime], which cause loss of money either to the bank or the customer, that is a really bad reputational risk. So that is why we would try to use some kind of alternative or try to downplay it…Insurance doesn't cover that much, so we just put it down as an operational cost. So far, touch-wood, that really hasn't happened frequently.*"[241]

[240] Transcript 9 (HK): p.2.
[241] Transcript 9 (HK): pp.2-3.

Another respondent, a director of an International Consultancy company working in the field of computer forensic and computer crimes in the Asia region, explained that:

> "*... probably first and foremost our clients are worried about the reputational damage. They might believe they have an issue with a member of staff or former employees but is not at the level which would be accepted by the police. Obviously the police have very strict acceptance criteria when they look at computer related crime, because of their resources limitation.*"[242]

He went on:

> "*Working in the private sector I am not so sure that our clients want to cover-up the extent of business fraud. I think it is more often the case that they actually don't know themselves to what extent, you know, to put a dollar value on fraud or Internet related losses. I think, certainly, publicly many organisations won't reveal losses, if they are aware of them, for a number of reasons: - reputational risk is a phenomenal risk to an organisation. I guess if a bank you know turns around and says they are losing 12m due to Internet fraud every year, it is going to knock the confidence of their customers to use their online banking services.*"[243]

Summary

As Tai has argued, since the late 1980s, the banking system in Hong Kong has been well regulated and closely supervised.[244] One of the reasons the HKMA keeps a watchful eye on the commercial banks is that bank-runs have had an adverse effect on the banking system in Hong Kong in the past. A bank has to fulfil a number of requirements before the HKMA will issue a banking licence.

[242] Transcript 1 (HK): p.3.
[243] Transcript 1 (HK): p.4.
[244] Tai, L.S.T. (1986) 'Commercial banking', in Scott, H.R., Wong, K.A. and Ho., Y.K. (eds.) Hong Kong's Financial Institutions and Markets. Hong Kong: Oxford University Press, p. 10.

These requirements were recommended in the Basel II accord[245] on banking supervision, which was fully implemented in Hong Kong during the late 1980s.[246] On paper, this should mean that the banks in Hong Kong are compelled to report any instances of crime to the police and the HKMA. However, the data collected in this thesis suggest that the banks (i) may not always be aware of Internet fraud; (ii) may seek alternative, informal solutions to the instances of fraud they are aware of; and (iii) tend, where possible, not to report such matters to the HKMA or the police if this there is a risk of reputational damage to the institution.

[245] The Bank for International Settlements (BIS) is based in Basel, Switzerland and currently employs 557 staff from 48 countries. See, <http://www.bis.org>. [Cited 24/05/2007].

[246] The Basel Committee was established by the central-bank governors of the Group of Ten Countries, comprising, Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States. According to the BIS website, representatives from these countries and subsequent additional member states meet four times a year. The Committee is not a formal supranational supervisory authority and their conclusions do not possess any legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them in ways that are best suited to their own national systems, in part to strengthen the internal and external controls of banks. Thus, the Committee encourages convergence towards common banking practices and standards without attempting dictate member countries supervisory techniques. See BIS, ibid.

# Chapter Five
# The Investigation

## Introduction

In this chapter, I examine what happens when a case of Internet banking fraud is reported to the police. Apart from the bank reporting an incident, a victim of Internet banking fraud can report the matter directly to the police, either in person, by phone, or via email or fax. In such cases, an initial investigation will be conducted by a frontline police officer, who has to decide whether to contact the bank or to record the incident as a crime. If the alleged Internet fraud is recorded as a crime, the police will assign a case reference number to the victim, contact the bank and require the victim to make an official report to their bank to prevent further losses. The police will conduct the investigation and the bank is required by the HKMA to co-operate with the police.

As Table 5.1 shows, Hong Kong's bank customers have been subject to a number of fraudulent emails and fake bank websites. These figures also indicate that the banks do report such cases to the HKMA and that the HKMA closely monitors the banks' crime statistics. These statistics also means that the HKMA and the banks can react quickly if the crime situation worsens.

**Table 5.1: No. of Reported Fraudulent Emails and Fake Bank Websites, 2003-2012**

| Years | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---|---|---|---|---|---|---|---|---|---|---|
| **Nos. of cases reported to HKMA** | 8 | 34 | 25 | 17 | 27 | 11 | 14 | 15 | 21 | 26 |

*(Source: HKMA. (28 April 2008) 'Briefing to the Legislative Council Panel on Financial Affairs, p.33 & HKMA website: <http://www.hkma.gov.hk/eng/key-information/press-release-category/fraudulent-websites-e-mails-and-telephone-system-and-other-fraud-cases.shtml>, visited 21/6/2013).*

How the Hong Kong Police Process Internet Banking Fraud

The first thing the police have to do after receiving a report of Internet banking fraud is to check whether a crime has actually been committed. If a bank reports a case of Internet fraud to the police, the police treat the incident seriously, regardless of the value, because they work closely with the banks and the bank's in-house investigator may already have completed most of the investigative work. This also makes it easier for the police to decide whether or not a crime has been committed. Moreover, the police are specially trained to know what to look for and officers at police stations across Hong Kong are trained to handle and deal with the victims of Internet fraud. When a crime is reported, these officers will know what to do next and how to record the crime correctly. Therefore, the fraud is likely to be properly recorded and investigated.

The Hong Kong police have developed a specialist unit to deal with cases of Internet fraud. Established in the early 2000s, the Technology Crime Initial Response Cadre[247] is made up of more than 80 officers with in-depth training in computer forensics, stationed all over Hong Kong. After receiving a report of a crime, members of the Cadre will examine the victim's computer for evidence of Internet fraud and check whether the law has been broken. The officers will then write an initial report on the case. A senior police officer will then decide whether to continue the investigation. If there is not enough evidence to continue the investigation, the case will be designated as 'No Further Action' and the incident will not proceed any further in the criminal justice process. If the police do decide to continue the investigation, the case may be referred to another specialist unit,

[247] The Information Service Department, (18/1/2001) Press Release. Hong Kong: Hong Kong Government

such as the Commercial Crime Bureau (CCB) and/or the Technology Crime Division (TCD). If they uncover further evidence to support the investigation, then the case will progress further; if not, it may be discontinued with 'No Further Action'. As a frontline police officer interviewed for this research said:

> "*Normally, if we uncover further evidence to support the reported case, ie. such as hard disk drives. etc…we will take further action and follow up with an investigation. If not, then the reported case would be passed onto another Unit at the CCB to follow up ie.'NFA' from TCD.*"[248]

The same police officer went on to describe the steps that the TCD has to take to secure the computer evidence to build the police case:

> "*Firstly, we will be applying for a search warrant from the court. In the court warrant application we will be listing out in detail the sort of equipment we are looking for, such as hard-disks, monitors, cables and mobile-phones etc... Once we got the warrant, we will go to the address in the court warrant and search for evidence. We will not touch any equipment but look at the equipment first, to see if there are any traps there. If no, then we will start to check the cables etc…then we will clone the hard-disk drive, floppy, USB…etc. When the cloning process is completed, we would seal all the cables, monitors, CPU, and all other evidence that supports the police case, with police evidence plastic and label it clearly with a unique reference number. This equipment will become CCB's property and it will be further examined by the computer forensics lab at CCB.*"[249]

The same officer went on:

> "*During the investigation, if we discover new types of … offence that we understand less, we will engage an outside technical expert to help us. Slowly we will learn from this technical expert. Nowadays, it is possible that a lot other multi-media could commit computer related crimes and contain computer evidence. To give an example, in a murder case, we might not know who the suspect is, but the victim could be communicating with*

[248] Transcript 5 (HK): p.1.
[249] Transcript 5 (HK): p.1.

> *the suspect through e-mail for some months already. Therefore, evidence can be found on the computer. via their e-mail accounts. Once we check the e-mail accounts and trace it back - so and so month, date, someone did actually communicate with the victim, and they both agreed to meet face to face, through these e-mails - we can find out the suspect's IP address and locate where the defendant was. One of best things about computers is that once an e-mail is sent to a server, it doesn't matter how many times you try to delete it, we could trace it back from the server's drive and find out what is going on. For most people, a delete is a delete, but the truth is we still can trace back the files and find the evidence by opening it with our forensics tools*"[250]

Another police office explained that:

> "*First of all, the Hong Kong Police has already established a division called the 'Technology Crime Division' (but internally we called it "Technical Crime Division"). This 'Technical Crime Division' is focused on technological crime. This is on the rise because, with technological advance in society, most Hong Kong enterprises are now using computers to operate their businesses. This is a good thing. People with high technological knowledge, they know how to protect themselves, but people with less technological knowledge, these people are less likely to know how to protect themselves and their computers with proper security. Therefore, computer related crime would likely happen to these people. The Hong Kong police, by establishing the TCD, focuses on technological crime and educates Hong Kong residents about this type of crime. When we receive a reported case, we first need to establish whether or not it is a technologically- related crime by speaking to the alleged victim, and find out what exactly has happened - whether it is a computer problem, or whether a third person has hacked into the computer, or whether someone has actually planted something into the computer which causes the victim to lose money. This is how we deal with the reported case. Well, if we discover that the alleged victim's computer was actually hacked/accessed by a third person, then we would investigate the case further. If not, then the reported case is passed onto another Unit, 'NFA from TCD'.*"[251]

The same police office added that:

[250] Transcript 5 (HK): p.2.
[251] Transcript 6 (HK): p.1.

"*In term of technological knowledge, not only as front line police officers, but as front line police officer in the TCD, technological knowledge is not a problem, because in TCD our technological knowledge and access to technological information is high. However, for other frontline police officers, the technological challenge may be greater, since in Hong Kong for the last 4 to 5 years, the technological advancement of the society has been at lightning speed. My other force unit colleagues, they may have been in the police force already 10 years or 20 years and their computer knowledge is not that high, so if these police officers handle computer related crime, from a TCD police officer's point of view, it is not too professional, because they do not have experience of dealing with computer related crime and are bound to made a lot of mistakes. In the end, TCD front line officers will be mopping up their 'dirt'. Furthermore, these police officers may have already reached 40 years of age. Like any other ordinary person in society, they themselves may be reluctant to learn new technological stuff. On the other hand, as a TCD front line police officer, we train to keep up with technology. Although we do train other colleagues in the police force in basic knowledge about computer crime evidence, when we arrive at the computer crime scene, TCD officers always remind these police officers not to touch any cables, equipment, keyboard and monitor in case any trap is there to erase or delete computer evidence. We [TCD officers] would check thoroughly before any computer related equipment is unplugged or plugged in. Basically, from a criminal point of view, technological related crime is like an arms race, since it needs a lot of modern technological equipment, instruments, in order for the police to secure the evidence. For example, a 12 inch PC and 12 inch Mac machine are different. It requires a unique cable and equipment to get the forensic evidence, so it all depends on how comprehensive your equipment is. The more instruments you have got, the faster we can seize the evidence. Therefore, at TCD we are constantly updating our software and equipment. Additionally, when we face a big computer network system, for this kind of computer network, at TCD we have a dedicated network team to handle big network computer forensics. But if we face some in depth network computer codes that we are not too sure about, or a very high level of hacking activities, TCD would engage a computer expert from a*

*local University to deal with it, together with an outside expert partner, to reconstruct the crime scene*."[252]

Bank-Police Liaison

An investigation is likely to require close liaison between the bank and the police. Since the 1970s, the banks and the police in Hong Kong, especially the CCB, have had a close working relationship. Co-operation with the law enforcement agencies is now second nature to the banks. For example, a tripartite Electronic Banking Working Group,[253] comprising representatives of the HKMA, the TCD and the Hong Kong Association of Banks (HKAB) was established in December 2002. The primary function of the group is to advise on consumer education and precautionary measures to enhance banking security, and provide guidance on reporting incidents of Internet banking fraud.[254] Importantly, the group also provides advice on intelligence sharing with the police on banking related crime. In mid-December 2002, the CCB held a workshop[255] on bank fraud, which was attended by forty-three senior security officers from 20 banks. During the workshop, the CCB outlined the details of Operation Tricot which had neutralised a syndicate perpetrating bank fraud crimes in November 2002. The fraud involved in exceed of HK$60 million. The three-day operation resulted in the arrest of 46 individuals, of whom 22 were core syndicate members who were subsequently charged with conspiracy to defraud and related offences. In addition to describing the arrests, the workshop outlined the significant intelligence

[252] Transcript 6 (HK): p.2
[253] See Hong Kong Monetary Authority, Banking Stability, (2002) Annual Report . [Online] [Cited 11/03/2007]. Available from: <http://www.info.gov.hk/hkma/ar2002/eng/policy_chapters/banking_progress07.htm>, p. 9.
[254] See Hong Kong Association of Banks. [Online] [Cited 12/03/2007]. Available from: <http://www.hkab.org.hk/asp/public/index.asp?Submit=AUs&lan=en>.
[255] See Hong Kong Police Force, (2003) 'Workshop on Bank Fraud', The Offbeat, Issue 744, January 22 to February 18 [Online] [Cited 12/03/2007]. Available from: <http://www.info.gov.hk/police/offbeat/744/eng/n09.htm>.

findings from the case, which serve as a good reference for identifying possible vulnerable areas in the banks' practices and preventing these vulnerabilities from being used in future.

The aim of the workshop was to update the banks on the latest modus operandi of bank fraudsters. The workshop also served as a forum for sharing best practice in combating this type of crime, especially, in regard to protecting weaknesses in the banking system and members of the police and the banking industry exchanged ideas for possible solutions. In closing the workshop, the commander of the CCB[256] expressed his appreciation to the bank security officers for their assistance throughout Operation Tricot. He added that this was a good example of a fruitful outcome achieved as a result of the close working relationship between the CCB and the banks. As a frontline officer interviewed for this research said:

> *"From my own experience, when investigating Internet banking fraud, it is essential that the bank co-operates with the police investigation, because we have to produce the proof that the money has indeed passed through the account in question.*
> *Interviewer: As a front-line officer, do you think that the communication between the banks and the Hong Kong police is smooth?*
> *Respondent G: It is okay; but the difficulty is that when the victim of fraud credits a certain amount of money into the perpetrator's designated bank account in Hong Kong, then possibly the money remains dormant for a long time, before the perpetrator enters Hong Kong and withdraws the money from the bank account. In this case, arresting the perpetrator would involve a certain level of difficulty.*
> *Interviewer: Do you think that there is a difference in terms of treatment between big banks and small banks by the Hong Kong Police?*
> *Respondent G: In my experience, the smaller banks are moving a little faster than the big banks, in terms of help. Maybe their workloads are smaller. Basically, when the*

[256] Chief Superintendent Wong Fook-Chuen.

*police request the bank's assistance, they [the bank] will just get on with it.*
*Interviewer: This is a very co-operative culture?*
*Respondent G: Never has been a problem. The banks are always courteous to us, but they need to see something in black and white before they can disclose any personal details of the account in question, I suppose, to protect their interests. Therefore, black and white is the key.*
*Interviewer: Is there any difference between international banks and local banks?*
*Respondent G: I personally think there is no difference between them. They always need to see the search warrant before they would disclose the account details in question. Maybe there is a little difference with the International banks on the presentation of details. Other than that, there is basically no difference and they will give you what you asked for. Maybe the big international banks would pay more attention to their appearance but, once you tell them what you want, they will quickly present it in front of you.*
*Interviewer: This is because the big bank has a specialist team to look after this kind of case?*
*Respondent G: You cannot say that. They probably have more chance to encounter Internet fraud cases, because they have more Internet bank account holders and the opportunity of fraud happening is greater. If it is a small local bank, since their Internet bank customer-base is small anyway, therefore, the chance of fraud happening is less.*
*Interviewer: In other words, the international banks have more experience in dealing with Internet banking fraud, than the smaller local banks?*
*Respondent G: "Yes, maybe. The smaller local banks have less experience."*[257]

Owing to their different levels of resources, international banks and local smaller banks have different approaches for dealing with police requests for assistance. The international banks have teams that deal specifically with Internet fraud, whereas the smaller local banks have fewer resources in this area because they are less likely to encounter Internet fraud in their daily business. Although both types of bank provide assistance to the police, the international banks are better

[257] Transcript 5 (HK) (In Chinese): pp.4-5.

equipped to deal with police requests because they have more experience and resources. As a Manager for Online Banking of a major global bank interviewed for this research explained:

> "*Obviously local banks, you know, they've gotta look at customer spread as well, compared to the risk level. The risk level is a bit different for them. I mean in their Internet composition, they may not have as many customer uptakes as a global bank. So, the risk level for them may be low or medium. Whereas for a big bank with bigger customer basis, we have a greater need to ensure that we invest in a state of the art technology.*"[258]

This same Manager added that:

> "*We are a global bank. We're also one of the largest banks in the world. Our internet related activities are also very large. Our presence in Hong Kong, our customer base here for internet banking is also quite high. So, you know, a lot of the external organisations come to us to work with us, and talk with our people, to also share experience, also learn from each other. So it's a two-way process really. But we have a very well-established procedure and organisation internally to tackle this area, and handle internet related frauds. The turnover is very quick, I'd say, we keep the regulators informed, so we have very good relations with the HKMA here in Hong Kong which I think is very important. So, this is how we handle this particular area…our IT security division is made up of, you know, people who know how these things work. They obviously monitor and watch how the systems…are 24/7, and any possibility of attempts to hack are stopped before they can even get through the system. I think we need constant monitoring because this area is constantly changing. There's always a new type of virus. There's a new type of style of hacking, software for hacking being introduced. So, our systems, our network, need to be robust enough to tackle all these new developments. So we have a very dedicated unit to look at this, and they prevent things like that happening. Regulation is regulation. We comply, you know. It's a legal requirement under the Electronic Transaction Ordinance. It is also required for legal evidentiary purposes. So we are fully complying with all those requirements. You know, our standards are*

[258] Transcript 3 (HK): p.3.

> *extremely high and we take this very, very seriously. Our role in the industry, our reputation, our position, in the industry is rated very highly. We would like to keep it that way. So, you know, we fully comply with the regulations.*"[259]

A specialist officer from TCD/CCB may visit the bank to check whether the law has indeed been broken. If the police accept that a crime *has* been committed, then they will investigate further. The TCD does not set a minimum monetary value on the computer frauds it investigates and will initially investigate every reported incident, large or small. The division generally treats any investigation of computer crime as a part of a learning process for their officers. As a Chief Inspector of TCD explained:

> *"Unlike other countries, other law enforcement agencies around the world, we do not set a minimum bar to taking up the computer investigation, in terms of the monetary values etc. That is because investigation of computer crimes in the HK police is still at a learning curve. So, even though the monetary values involved in a crime may be very low, it does not reflect the resources that we are putting in. We look at it as a sort of learning process that our officers gain from it. Basically, we take up any report of computer related crime in HK.*"[260]

Summary

On the whole, the Hong Kong police are well resourced to combat Internet economic crime and other technologically-related crimes. Because of the high level of resourcing in this area, the police are able to post technologically-trained frontline officers in local police stations across the territory and provide high levels of funding to specialist officers. As a result, the Hong Kong police have a high level of force capability in regards to Internet banking crime. The fact the

[259] Transcript 3 (HK): pp.1-2.
[260] Transcript 8 (HK): p.1.

police are so well resourced and trained also reflects the government's policing priorities. Banking is one of the pillars of Hong Kong's service industry and is central to Hong Kong's international reputation as a financial centre. Accordingly, protecting and maintaining Hong Kong's 'clean' financial system is a key government policy. The current policing priorities and resources reflect this need to concentrate on economic crime, while tradition and the close inter-relationship between government and business has led to a close liaison between the banks and the police when it comes to the investigation of Internet banking fraud.

# Chapter Six
# The Law

Introduction

Only a very small number of computer crimes proceed to trial in Hong Kong (see Table 6.1 below). In this chapter, I examine whether this is related to the law, specifically the Computer Crimes Ordinance 1993, which allows the police to change a computer related charge to another offence during the prosecution process. Thus, while a case may enter the criminal justice process as an offence charged under the Computer Crimes Ordinance, the defendant may end up being tried for a different offence (for example, see Case 2 in the sample of cases, below).

**Table 6.1: Nos. of Trials for Technology Related Crimes**

| Years | 2003 | 2004 | 2005 | 2006 | 2007 |
|---|---|---|---|---|---|
| **Advices to TCD/CCB (Cases)** | 44 | 50 | 41 | 41 | 32 |
| **Trial** | 10 cases (8 persons convicted) | 15 cases (18 persons convicted) | 17 cases (15 persons convicted) | 15 cases (11 persons convicted) | 21 cases (20 persons convicted) |

*(Sources: The Department of Justice Yearly Review 2003; 2004; 2005; 2006; 2007)*

In total, 205 trials for technology-related crimes were held between 2003 and 2007. Some of the cases also had an economic crime element and most were heard in the Magistrates' Court. As such, these types of cases are generally not reported in the Law Reports.

What to Charge: How does the Law Shape Police Investigation and Prosecution?

The Computer Crimes Ordinance 1993 is the main piece of legislation on computer related crime. According to a report by the Hong Kong inter-departmental working group on computer related crime, the Computer Crimes

Ordinance was instituted by amending existing laws and creating some new offences to broaden the coverage of the existing legislation. Hong Kong's computer related crime legislation is now sufficiently flexible to cover both the physical and the virtual worlds.[261] Furthermore, the police have considerable flexibility in making charges. For instance, they can charge a case of Internet banking fraud as (i) traditional theft under the Theft Ordinance (Cap. 210); (ii) fraud under the section 16A of the Theft Ordinance (Cap. 210); or iii) as a combination of six offences stipulated under the Computer Crimes Ordinance 1993. In this chapter, I examine the repercussions, if any, that this flexibility has on the charging and prosecution of Internet banking fraud in Hong Kong? As a frontline police officer interviewed for this research said:

> "*In Hong Kong, the computer crime law, which is the 'Computer Crimes Ordinance 1993' is quite sufficient. It is flexible enough for us to work with, at the initial charge stage and at court.*"[262]

i). Charging the Recorded Crime as Theft under the Theft Ordinance (Cap. 210)

The basic definition of theft, provided in Section 2 (1) (2) of the Theft Ordinance, is as follows:

> *"(1) A person commits theft if he dishonestly appropriates property belong to another with the intention of permanently depriving the other of it; and 'thief' and 'steal' shall be construed accordingly.*
>
> *(2) It is immaterial whether the appropriation is made with a view to gain, or is made for the thief's own benefit.*"

[261] See Inter-department Working Group on Computer Related Crime Report, September 2000, Hong Kong: Hong Kong Government, pp.5-8.
[262] Transcript 6 (HK): p.4.

The Theft Ordinance requires the prosecutor to prove that the defendant has dishonestly appropriated the property of another. This is part of the *mens rea*. The definition of 'appropriation' in section 4 of the Theft Ordinance is the same as that in section 3 of the Theft Act 1968. In terms of case law, for *actus reus* in general, the Hong Kong Court of Appeal follows the House of Lords' decision on *Gomez*[263], affirmed in *Hinks,*[264] in regard to the interpretation of 'appropriation'.

To establish proof of *mens rea* in theft, the Hong Kong Courts also follow the English courts, which require proof that the defendant (i) acted dishonestly and (ii) with the intention of permanently depriving the owner of the property. This means that to bring a charge under the Theft Ordinance, the Hong Kong police need to establish i) appropriation, ii) that the property belonged to another, iii) that the defendant intended to permanently deprive the other of the property, and iv) that the property was dishonestly appropriated.

Because the structure of the Theft Ordinance is very complex, establishing the guilt of an offender is a complicated task for the police. However, because the ordinance includes the option of charging fraud as a general fraud offence under section 16A, the police in Hong Kong have an easier job in charging and investigating Internet banking fraud (see **Cases 4** and **14** in the case sample, below). Section 16A was inserted into the Theft Ordinance in 1999. Hong Kong has also introduced its own specific fraud law,[265] which was established by

[263] *R v Gomez [1993] AC 442.*
[264] *R v Hinks [2001] 2 AC 241.*
[265] The government was prompted to introduce a specific fraud law in Hong Kong in the early 1980s, when numerous scandals involving financial institutions were uncovered. This was partly to do with a dramatic growth in the number of banks and deposit taking companies (DTC) registered in Hong Kong, which led to increased competition to lend to customers. The DTC did

amending section 16A of the existing Theft Ordinance (Cap. 210). Section 16A of Theft Ordinance provides a basic definition of fraud as follows:

---

not come under the Banking Ordinance and were left unregulated until 1976, after which their number dropped dramatically. According to Schenk, the moratorium on new bank licences was lifted in 1978 and, by 1982, the number of licenced banks increased from 74 to 128. At the same time, the number of banking offices almost doubled from 759 to 1474, and the number of DTCs increased from 179 to over 350. See Schenk, C.R. (July 2003) 'Banking Crises and the Evolution of the Regulatory Framework in Hong Kong', Australian Economic History Review, Vol.43, No.2, p.12. These financial companies made loans to some customers whose credit-worthiness was less secure, much of it relating to property speculation. In 1982, as a result of spiralling interest rates, many customers were unable to service their loans. At the same time, the asset value of their securities took a nose dive, followed by the collapse of the property market. Inevitably, insolvencies were incurred. Consequently, a number of local banks and DTC were hit with sudden liquidity problems and collapsed. However, some of the banks were rescued by the Hong Kong government with public money, which caused public outcry over the cost. The government took the view that the failure of the banks would affect the Hong Kong dollar under the circumstances prevailing at that time. Consequently, these banks were rescued by the Exchange Fund, whose main role was to maintain currency stability. According to Li, from 1983 to 1986, seven local banks got into difficulties. These included the then third largest local bank in Hong Kong, the Overseas Trust Bank. Three of them were taken over by the government and provided with financial assistance in the form of a guarantee of assets and liquidity support. With the other four, the government facilitated takeovers by private sector entities. See Li, R. 'Banking Problems: Hong Kong's Experience in the 1980s', Executive Director, Banking Policy Department, Hong Kong Monetary Authority, pp. 131-132. After the government investigation, fraud was suspected in certain cases, according to the Law Reform Commission of Hong Kong. For example, the property developer Carrian collapsed after it was discovered that it was fraudulently financed by a DTC called Bumiputra Finance, a subsidiary of a state-owned bank in Malaysia. However, problems arose in the prosecution of these fraud cases. Suspects were absent from Hong Kong, often living in countries from which extradition was not possible. Furthermore, even in those cases where the suspects were in countries from which they could be extradited, the terms of the relevant extradition treaties might mean that a charge of conspiracy to defraud could not be laid. As the Law Reform Commission sub-committee stated, "*the [Extradition] Treaty lists fraud as a separate offence, but since Hong Kong does not presently have a substantive offence of fraud, extradition cannot be obtained under this heading. Conspiracy is only extraditable if it is conspiracy to commit a substantive offence listed in the [Extradition] Treaty*." Even if suspects were arrested in Hong Kong, there could be problems with the charge of conspiracy to defraud, the length of the trials and the question of bail. Then, in May 1988, the Law Reform Commission appointed a sub-committee to consider and advise on the present state of fraud law and to make proposals to the Law Reform Commission. The sub-committee concluded in its report that there was a need for a new substantive offence of fraud but that this should be restricted to circumstances where there had been a scheme of fraud. Subsequently, the Commission itself, in July 1996, reported on the creation of a substantive offence of fraud and concluded that the problem should be looked at afresh, laying particular emphasis on an examination of the law in those jurisdictions that already possess a substantive offence of fraud, such as Scotland and South Africa. The Commission's conclusion was that a substantive offence of fraud should be introduced in Hong Kong. Two years later, on 5 January 1999, the government tabled the Theft (Amendment) Bill 1998 for the Legislative Council Bills Committee to examine. The government proposed in the new Theft (Amendment) Bill to create a new substantive offence of fraud and retain the common law offence of conspiracy to defraud. The Legislative Council Bills Committee held seven sessions, before passing the new Theft (Amendment) Bill onto the main chamber of the Legislative Council for debating and voting. The Bill was eventually passed and became the Theft (Amendment) Ordinance (45 of 1999) in July 1999.

> *"(1) If any person by any deceit (whether or not the deceit is the sole or main inducement) and with intent to defraud induces another person to commit an act or make an omission, which results either-*
> *(a) in benefit to any person other than the second-mentioned person; or*
> *(b) In prejudice or a substantial risk of prejudice to any person other*
> *than the first-mentioned person, the first-mentioned person commits the offence of fraud and is liable on conviction upon indictment to imprisonment for 14 years.*
> *(2) For the purposes of subsection (1), a person shall be treated as having an intent to defraud if, at the time when he practises the deceit, he intends that he will by the deceit (whether or not the deceit is the sole or main inducement) induce another person to commit an act or make an omission, which will result in either or both of the consequences referred to in paragraphs*
> *(a) and (b) of that subsection."*

The type of case that could fall under section 16A, might include the following. For example, C and D set up an Internet trading company, which they operate for some months, during which time they establish relationships and business trust with several suppliers. C and D then place several large orders with the suppliers. The suppliers deliver the goods on credit. C and D then sell the goods via their Internet website, take the money, close down the website and disappear. Before the enactment of section 16A, the police had two options in charging such a crime. First, they could have charged C and D with conspiracy to defraud under the common law, which would require proof of at least two co-conspirators who had a prior agreement to defraud. However, even though the fraudulent scheme had been perpetrated and the suppliers defrauded, it would have been difficult for the police to gather evidence to prove the case, because it would have been very difficult to establish the *mens rea* of the co-conspirators. As an alternative, the police could have charged C and D with deception under the Theft Ordinance.

After the enactment of the general fraud offence, such cases became easier to establish. First, the offence under section 16A uses the concept of 'deceit' instead of 'deception. According to the Law Reform Commission,[266] 'deceit' was adopted in formulating the offence of fraud because "*it is the element of deceit which is the key feature which distinguishes fraud from theft*". Moreover, the report stated that requiring deceit would be a "*departure from the House of Lords finding in the Scott case, that deceit was not an essential element of fraud.*" In *Scott v Metropolitan Police Comr. [1975] AC 819*, the Law Lords held that fraud depended on the proof of dishonesty, not deceit. The Hong Kong Law Reform Commission wanted to avoid the problems associated with the English common law proof of dishonesty in fraud in *Scott*. According to Jackson, the Hong Kong legislators preferred to formulate an offence of fraud in terms reflecting the principle accepted in *Re London and Globe Finance Corporation, Limited [1903] 1 Ch. 728*[267], to the effect that it is deception rather than dishonesty which is the key consideration in fraud.

Secondly, section 16A does not expressly require proof of dishonesty. To prove *actus reus* under section 16A (1), the police are simply required to prove that a person has used deceit to induce another to commit an act or make an omission and that the person benefits from, makes financial gain or poses a substantial risk of prejudice to someone other than the person practicing the deceit. For *mens rea*,

[266] The Law Reform Commission of Hong Kong Report on fraud, para.5.25.

[267] *RE London and Globe Finance Corporation, Limited [1903] 1 Ch. 728* at 732-733: "*To deceive is, I apprehend, to induce a man to believe that a thing is true which is false, and which the person practising the deceit knows or believes to be false. To defraud is to deprive by deceit: it is by deceit to induce a man to act to his injury. More tersely it may be put, that to deceive is by falsehood to induce a state of mind; to defraud is by deceit to induce a course of action*." See Jackson, M. (2003) Criminal Law in Hong Kong. Hong Kong: Hong Kong University Press, p. 770.

the police must prove that a person has deliberately or recklessly made a false representation amounting to deceit, by proving that the person intended to deceive or induce the victim to act in a manner resulting in financial or proprietary benefit or prejudice. As Jackson says, "*section 16A (1) now offers a much simpler way of prosecuting the fraudulent scheme*".[268]

Section 16A of the Theft Ordinance covers various types of fraud, including traditional fraud and non-traditional fraud, such as Internet banking fraud. Overall, the introduction of a specific general fraud offence, the simplification of the law on fraud and the abandonment of the English common law proof of dishonesty have made it easier for the police to gather evidence on and prove cases of fraud. As a result, the police are now more likely to charge offenders under section 16A of the Theft Ordinance.[269]

ii). Charging a Recorded Crime under the Computer Crimes Ordinance 1993

Prior to the enactment of the Computer Crimes Ordinance in 1993, the Hong Kong police typically applied the traditional law to computer related crimes. The

[268] Jackson, M. (2003) Op Cit: p. 769.

[269] The following are examples of some of the police charges under section 16A: on 5 July 2000, in a case concerning a director of a Malaysian-based Hong Kong securities company, four accounts were found to have an unsettled outstanding balance of over $6.4m. Subsequently, it was discovered that the director had been using the money, without the company's consent, to repay personal debt since 1988. The company reported him to the Commercial Crime Bureau. He was arrested by the police and charged with four counts of fraud under section 16A of the Theft Ordinance. Later, he pleaded guilty to these charges at the District Court and was sentenced to 42 months imprisonment. In another case, *HKSAR and William Cole CACC 488/2005,* the defendant was charged under section 16A of the Theft Ordinance with fraud for misusing someone else's credit card on twenty-four occasions. He was convicted in the District Court and was sentenced to 4 years imprisonment. Cole appealed the conviction. In the appeal, he argued that he was wrongly charged under section 16A. However, the appeal was dismissed by the Court of Appeal. In another case, *HKSAR and Tsang Kwok Wing and Lee Kwok Cheong CACC 406/2006*, car park attendants Lee and Tsang were charged with falsely representing their attendance records at car parks managed by Kwik Park Ltd with intent to defraud or to deceive over a 3 year period between 3 April 2001 and 27 May 2004. When the case was heard on 8 September 2006 at the District Court, Tsang was convicted on five charges of fraud contrary to section 16A of the Theft Ordinance and Lee was convicted on two charges of fraud under section 16A. They appealed their convictions, but the Court of Appeal dismissed their applications.

Computer Crimes Ordinance, which was largely modelled on the UK Computer Misuse Act 1990, primarily aimed to criminalise hacking, dishonesty and theft within the computing environment. However, the Hong Kong Computer Crimes Ordinance differs from its UK counterpart in a number of ways. In particular, it criminalises more offences than the UK Computer Misuse Act.

The Computer Crimes Ordinance was one of the first laws specifically designed to tackle the misuse of computers to be introduced in Asia. The new ordinance amended relevant sections of existing legislation to cover computer crime. For example, the ordinance added new sections to the Telecommunication and Crimes Ordinances (see below) and amended provisions in the Theft Ordinance (see below). Other provisions in the Crime and Theft Ordinances were also amended to make it clear that offences such as false accounting, forgery and making a false entry in a bank book also applied to information stored in a computer.

The Computer Crimes Ordinance 1993 is divided into six sections: (i) section 27A of the Telecommunication Ordinance (Cap. 106), (ii) sections 59 and 60 of the Crimes Ordinance (Cap. 200), (iii) section 85 of the Crimes Ordinance (Cap. 200), (iv) section 161 of the Crimes Ordinance (Cap. 200), (v) section 11 (3) of the Theft Ordinance (Cap.210) and (vi) section 19 of the Theft Ordinance (Cap.210).

(i). Section 27A of the Telecommunication Ordinance (Cap. 106)

Section 27A of the Telecommunication Ordinance (Cap. 106) provides the basic definition of unauthorized access to computer by telecommunications ('hacking') as follows:

> *"(1) Any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $20000. (Amended 36 of 2000 s. 28)*
> *(2) For the purposes of subsection (1)-*
> *(a) the intent of the person need not be directed at-*
> *(i) any particular program or data;*
> *(ii) a program or data of a particular kind; or*
> *(iii) a program or data held in a particular computer;*
> *(b) access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and-*
> *(i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;*
> *(ii) he does not believe that he has been so authorized; and*
> *(iii) he does not believe that he would have been so authorized if he had applied for the appropriate authority."*

Section 27A of the Telecommunication Ordinance creates a basic offence to criminalise any form of hacking. Here, the requirement on the police to prove *actus reus* under section 27A is the same as in Section 1 (1) of the UK Computer Misuse Act 1990. For example, as in the UK, any person who gains unauthorised access to a computer system is guilty of an offence under section 27A if the police can prove that there was intent to hack into the person's computer.

(ii). Sections 59 and 60 of the Crimes Ordinance (Cap. 200)

Together Sections 59 and 60 of the Crimes Ordinance (Cap. 200) provide the basic definition of damage or modification of computer data.

> Section 59 provides the definition for computer property:
>
> "*(1) In this Part, "property" means-*
> *(a) property of a tangible nature, whether real or personal, including money…*
> *(b) any program, or data, held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature."*
>
> Section 60 provides the definition of destroying or damaging computer data or property:
>
> *"(1) A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.*
> *(2) A person who without lawful excuse destroys or damages any property, whether belonging to himself or another-*
> *(a) intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged; and*
> *(b) intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be thereby endangered, shall be guilty of an offence.*
> *(3) An offence committed under this section by destroying or damaging property by fire shall be charged as arson."*

Putting these two sections together creates the basic offence of damaging computer data or its content. The majority of the section is different to section 3 of the CMA 1990. Section 60 also covers the offence of unlawful modification of computer data or contents, which is similar to section 3 of the Computer Misuse Act. For example, if a person legally or illegally logs-in to a computer system and destroys or modifies any data file within the computer system which does not

belong to him or her, he or she will have committed an offence under section 60 of the Crimes Ordinance.

(iii). Section 85 of the Crimes Ordinance (Cap. 200)

Section 85 of the Crimes Ordinance provides a basic definition of defrauding a banking account as follows:

> "*(1) Any person who, with intent to defraud-*
> *(a) makes any false entry or alters any word or figure in any of the books of account kept at any bank in Hong Kong or by any body corporate, company or society, established by charter or by, under, or by virtue of any Ordinance, in which books the accounts of the owners of any money deposited in such bank or of any stock of any such body corporate are entered and kept; or (Amended 13 of 1999 s.3)*
> *(b) in any manner falsifies any of the accounts of any such owners in any of the said books; or*
> *(c) makes any transfer of any share or interest in any such deposit or stock in the name of any person not being the true and lawful owner of such share or interest, shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for life."*

In this case, section 85 criminalises any person who defrauds a bank account, makes a false book entry or illegally acquires stocks and shares for their own gain or for the gain of others commits a crime. For example, if a bank's employee simply alters or makes a false entry in a client's bank account via an internal or external computer system, he or she will have committed fraud under section 85 of the Crimes Ordinance.

(iv). Section 161 of the Crimes Ordinance (Cap. 200)

Section 161 of the Crimes Ordinance provides the basic definition of unauthorised access to a computer system with criminal or dishonest intent to commit further crime as follows:

"*(1) Any person who obtains access to a computer-*
*(a) with intent to commit an offence;*
*(b) with a dishonest intent to deceive;*
*(c) with a view to dishonest gain for himself or another; or*
*(d) with a dishonest intent to cause loss to another,*
*whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years."*

Section 161 aims to criminalise unauthorised access with intent to commit further serious crime, such as dishonesty, fraud and theft. As in section 2 of the Computer Misuse Act 1990, under section 161, the police can infer that a person has accessed a computer system with intent to commit a serious crime if that person uses someone else's password and pin number to access the computer system. All the police have to prove is whether or not the hacker accessed the computer account. However, the police may still have to prove some other intent. (**Cases 1, 2** and **3** in the case sample were indicted under section 161).

(v). Section 11 (3) of the Theft Ordinance (Cap.210)

Section 11 (3) of the Theft Ordinance makes it an offence to enter a building and tamper with a computer inside:

*"(3) References in subsections (1) and (2) to a building shall apply also to an inhabited vehicle or vessel, and shall apply to any such vehicle or vessel at times when the person having a habitation in it is not there as well as at times when he is.*
*(3A) The reference in subsection (2)(c) to doing unlawful damage to anything in a building includes-*
*(a) unlawfully causing a computer in the building to function other than as it has been established by or on behalf of its owner to function, notwithstanding that the unlawful action may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;*
*(b) unlawfully altering or erasing any program, or data, held in a computer in the building or in a computer storage medium in the building; and*

> *(c) unlawfully adding any program or data to the contents of a computer in the building or a computer storage medium in the building."*

Section 11 (3) of the Theft Ordinance criminalises anyone who has entered a building legally or illegally and alter the contents of a computer system. If a person enters an office in Hong Kong and sees a computer system that has already been logged-into and then changes some of the computer's contents and saves the files, they will have committed an offence under section 11 (3).

(vi). Section 19 of the Theft Ordinance (Cap.210)

Section 19 of the Theft Ordinance provides a basic definition of making a false entry to a computerised accounting system as follows:

> *"(1) Where a person dishonestly, with a view to gain for himself or another or with intent to cause loss to another- (a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or (b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular, he shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for 10 years.*
> *(2) For the purposes of this section a person who makes or concurs in making in an account, record or document an entry which is or may be misleading, false or deceptive in a material particular, or who omits or concurs in omitting a material particular from an account, record or document, is to be treated as falsifying the account, record or document.*
> *(3) For the purposes of this section, "record" includes a record kept by means of a computer*."

Section 19 of the Theft Ordinance criminalises any person who makes a false accounting entry for personal gain or the gain of others. For example, if a person

makes a false entry in a computerised book-keeping system, he or she commits an offence under section 19.

Summary

Overall, as the above shows, the Hong Kong police have a range of different options for charging cases of Internet banking fraud. In particular, they are able to charge someone under various ordinances other than the Computer Crimes Ordinance, because these ordinances have all been amended to include computer misuse offences. For example, the Theft Ordinance has been amended to include a section covering theft by computer misuse. This means that the police can charge a person with theft using the existing law, which now covers theft in a computing environment. For example, HKImail[270] reported that on 5 February 2001, a 39 year old man was charged and jailed in a landmark case for theft of HK$250,000 from a woman's Internet bank account. Tang Kwong-Wing was sentenced by the Eastern Magistracy to 20 months imprisonment after being found guilty of three counts of theft and two counts of attempted theft on the Internet. This was the first Internet theft case in Hong Kong in which a defendant was prosecuted and sentenced for stealing money through an online banking account.[271]

It also appears that the police can use the Computer Crimes Ordinance as an administratively convenient 'catch all' charge by which to begin an investigation.

[270] Lee, M. (06/02/2001) 'online banking thief gets 20 months'. Hong Kong: HKImail, p. A5.
[271] Tang found the victim, Ms Fu's, bank book containing her account details. Fu made a report to the police after finding HK$250,000 had been transferred from her account without her consent. One month later, Tang was arrested after TCD investigators' found the bank book and linked Tang's Internet bank account to Fu's bank account details.

However, the offender may be charged with further and different types of crimes (possibly more serious) as the investigation proceeds and evidence is uncovered.

Because cases of Internet banking fraud may be prosecuted as theft or other offences, it is difficult to tell from the official reports which cases of fraud are actually Internet-related. Similarly, the official crime statistics may classify an activity as theft or another offence, even though it involves Internet banking fraud. As a result, it is difficult to determine how many cases of Internet banking fraud have been committed, which may also explain the low number of recorded crimes in this area.

# Chapter Seven
# Police Investigatory Issues and Skills

## Introduction

This chapter examines the kinds of problems faced in policing Internet banking fraud and the ways in which the Hong Kong police and related agencies have responded to these challenges.

## Multi-jurisdictional investigations

As Smith and Urbas state, most electronic fraud does not involve face-to-face communication.[272] Internet crime is also often international and it is possible for offenders and victims to be located in more than one jurisdiction. This makes the investigation and prosecution of such crimes complicated. Hong Kong is also particularly prone to multi-jurisdictional policing problems. There are a number of reasons for this. First, because Hong Kong is a major financial centre in southern East Asia, criminals from overseas often target the Hong Kong banking system. As a senior computer crime prosecutor from the Department of Justice interviewed for this thesis said, "*Hong Kong is a very important commercial centre and there is lots of room for E-fraud*".[273] Second, people in Hong Kong are more mobile than in many other cities or countries. Historically, when Hong Kong was still a British colony, Hong Kong was known as a 'stepping-stone' to other places. In addition, many Hong Kong people aspire to emigrate to the United States, Canada, Australia, Europe and other countries in South Asia to secure a better livelihood for their family. As a result, Hong Kong migrants have

[272] Smith, R.G. and Urbas, G. (2001) Controlling Fraud on the Internet: A CAPA Perspective, Australian Institute of Criminology Research and Public Policy Series No. 39, KL: CAPA, p. 77.
[273] Transcript 2 (HK): p. 4.

built extensive overseas networks, which now increasingly rely on the Internet to communicate and to transfer funds. Third, Hong Kong is a free-port. To facilitate the free-port economy, minimal formality is required for goods and services entering and exiting the Hong Kong border. As a result, there are few or no restrictions on the financial flows between Hong Kong businesses and their overseas partners. Hong Kong is also the third largest foreign exchange market in Asia, with foreign exchange transactions reaching US$175 billion[274] in 2007. Internet banking is the most popular channel for banking services, with penetration increasing from 23 per cent in 2003 to 43 per cent in 2006.[275] As a detective chief inspector of the TCD stated in an interview for this research said: *"[in] financial investigations, there are obviously a lot of cases which are overseas…look at the technology crime itself, uh, it is roughly I would say that about 1/4 to 1/3 of our cases would somehow relate to overseas…"*[276] (**Case 7** in the case sample is a case in point).

The international nature of Internet related crime poses cross-jurisdictional issues for the police. If evidence is located outside Hong Kong, the TCD can make an informal approach to officers in the other jurisdiction, make a formal request for assistance or just simply discontinue the investigation. As Smith and Urbas[277] have suggested, most problems in extraterritorial law enforcement relate to cost and delay, which can make some prosecutions practically impossible.. As a frontline police officer interviewed for this research said:

[274] Hong Kong Trade Development Council (HKTDC). [Online] [Cited 3/11/2008]. Hong Kong: Hong Kong Government. Available from: < http://info.hktdc.com/main/economic.htm>.
[275] Sullivan, P. (2 April 2007) 'Panel on Financial Affairs-Legislative Council'. Hong Kong: HKAB.
[276] Transcript 4 (HK): p. 3.
[277] Smith and Urbas (2001) Op Cit.: p. 78.

> "*If the computer crime happened inside Hong Kong, it is much easier for us. We simply request the Hong Kong ISP to co-operate with us, and they are always happy to co-operate with us. For computer related economic fraud, we just go to the ISP's server to collect the evidence, such as the IP address. All of this can be done quite easily in Hong Kong, But if the reported case involves an international element, that is a different story. At the moment, international co-operation is ok with various police co-ordination centres in Asia and Interpol. However, it depends on the timing of the case. In some cases, we have to give up the case because different countries have differences in their laws. For example, in some countries, even when approached for help, the ISP operators ask for an administrative fee before they answer your e-mail/ phone calls, or in some countries their prosecutor is not trained in computer related crime. They do not even know how to approach the ISP operators in their search warrant application. They basically do not understand what computer evidence is. But in Hong Kong, we do not have this kind of issue. At the DOJ we have got a team of prosecutors who are well trained in computer related crime. If this is the case with some overseas computer crimes there is nothing TCD can do about it. With frustration we 'give up*"'.[278]

A Chief Inspector of TCD interviewed for this research echoed this view:

> "*With overseas computer fraud, yes there is an MLA treaty to get information from overseas, but we need to go through the court proceedings, as part of the MLA process. The quickest one, from my experience, is between three months to six months. So trans-jurisdictional matters are a problem. If the crime happened in the country that has signed the [MLA] treaty, the member country cannot turn-down our request for getting the evidence. In fact, we are quite self-disciplined. We know if reported cases don't have a chance of getting through our Department of Justice, if there is not a serious crime or if it only involves a very small monetary value. Basically, it is not because we don't want to investigate the crime, but it is not in the public interest to investigate the crime. Another situation is where the crime is a crime in the country where it is committed, but in the country that you want get the evidence from, it is not a crime. The most common*

[278] Transcript 6 (HK): pp.3-5.

> *example of that is pornography. In Hong Kong, it is classified as indecent or obscene, but often it is not a crime in the Western country. When you try to get the evidence, your counter-part overseas cannot help with it.*" [279]

Smith and Urbas also state that a number of initiatives were introduced to address Internet crime in the Asia-Pacific region the 1990s.[280] For example, a working group was established on information technology crime to assist the Interpol Steering Committee on Information Technology Crime. An expert group on crimes related to computer networks was also set up, chaired by the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders. As a result of these initiatives, regional computer-related crime can be addressed by the authorities within the Asia-Pacific region, which eases the problem of collecting electronic evidence within the region. When a formal approach is made to recover trans-border evidence, the police can also approach Interpol for assistance. In theory, a suspect apprehended overseas can be extradited to Hong Kong for trial. However, as a police officer in the Technology Crime Division stated in an interview for this thesis, "*If the offender is located overseas, then it is very difficult to arrest the perpetrator*."[281]

On the problems of multi-jurisdictional e-crimes, a Police Chief Inspector of the Technology Crime Division interviewed for this research said:

> "*People can commit crime over the Internet in many places around the world. They could log-on to the [computer] machine in place A and then access place B and then make their financial transaction in place C, so you are relying on information from multiple*

[279] Transcript 8 (HK): pp.5-6.
[280] Smith and Urbas (2001) Ibid.
[281] Transcript 5 (HK) (In Chinese): p.4.

> *jurisdictions. Compare this with traditional street crime, where most likely you are involved in just one or two places. Over the Internet, I mean there are millions of geographical locations, because it could be anywhere. So there's no point to just pinpointing, say one particular place or another place, because people can kind of hop from one place to another. So, unless you can find the first port of contact, by providing that information then we can look for the second hop, third, fourth and fifth. Then finally we can identify the source of the attack and these are the problems that we do encounter.*"[282]

He went onto explain some of direct experiences the police have received when requesting of out of jurisdiction case assistant:

> "*in some situations, the overseas [police agencies] may think, oh this is internet google, less than a HK$1000, only a couple of hundred dollars [a little more of one hundred US Dollars], they will consider that this is a low priority, and they will be slow in response to our request for information, because obviously they must be overloaded with other cases as well.*"[283]

This point was also made confirmed by a team leader of a computer crime and forensic unit in a major global international management consultancy group in an interview for this research. The Head of the Asia region and a former member of the UK's police force, he noted that:

> "*In multi-jurisdiction cases, you only catch the culprit if you know just where your evidence is actually stored. It may be that a system is being hacked in Australia, but your offender is in Tokyo. I recently did an investigation, a virus incident, where a virus was introduced to an organisation in Australia, but it was actually being introduced by somebody working in a satellite document [i.e. remote access] in Tokyo and obviously there is a huge physical gap between Australia and Tokyo.*"[284]

[282] Transcript 4 (HK): p.4.
[283] Ibid.
[284] Transcript 1 (HK): p.4.

In addition to the cross-jurisdictional problems, out of jurisdiction Internet crimes are also costly and take a long time to investigate. As a Police Chief Inspector of the Technology Crime Division interviewed for this research explained:

> "*Firstly, the [the Internet fraudsters] may be all overseas. It's expensive to fly them over and it is expensive for the victim to fly over. Secondly, basically it's the costs involved in investigating such cases which is the main issue. Thirdly, in some other cases, you identify the culprits, how they set up certain websites, set up certain web-mails. So they are set up in some country where the law enforcement, does not have the capability to investigate computer crime and it is very difficult to locate the culprits as well."* [285]

Nonetheless, such cases are more likely to be investigated in Hong Kong than in other jurisdictions, because the Hong Kong police pursue all types of financial crime, whether serious or minor, as a matter of public policy. Furthermore, most of the major international banks have regional headquarters in Hong Kong. If these banks become a target of a fraud, they can investigate the matter themselves by seeking information from their global networks. As a manager for online banking of a major global bank interviewed for this research said:

> "*We don't sit and wait until it happens to us. We have a very robust system that we're confident in. We have a dedicated IT security division who also look at this area. So when any incident happens, it involves the collective effort of a lot of divisions within the bank. And within those divisions, we have experts who would have looked at these types of cases. And we have relations with external organisations, such as the police, the regulators, government bodies, industry bodies, whom we work with too. So, that helps us, before it escalates to a certain level.*"[286]

[285] Transcript 4 (HK): p.4.
[286] Transcript 3 (HK): p.1.

These banks can also provide vital evidence to the police in multi-jurisdictional cases. Even so, banks in some other jurisdictions do not routinely co-operate with the police and may not hand the necessary evidence on to the police even if they collect it (see **Case 7** below).

Specialist Units

As Internet banking fraud is often technologically and financially complex, it poses particular challenges that the police generally do not face when dealing with everyday types of 'real time' crime. As mentioned above, members of the police technology crime cadre[287] are specially trained to carry out such investigations. As Respondent 4, a senior officer of the TCD, said:

> *"Basically we…uh…we have over 150 what we call the TCIRC, Technology Crime Initial Response Cadre. These are the police officers that have received the basic training. Some of them have passed the basic training and they are selected for mass training. So they have a better knowledge of dealing with computer exhibits at the scene of crime. They'll be able to give advice to other traditional crime officers about how to handle computer related crime. So, that's the frontline officers. We provide them with the training so that they could then be able to help other frontline officers to deal with computer related crime*." [288]

[287] The cadre are based within local police stations, under the command of the regional police formation. The six regional police formations in Hong Kong are Hong Kong Island, Kowloon West, Kowloon East, New Territory South, New Territory North and Marine.
[288] Transcript 4 (HK): p.1.

Searching for Evidence

Investigating and gathering computer evidence clearly requires a great deal of technological and financial expertise. According to a police frontline officer of the Technology Crime Division interviewed for this research:-

> *"[when we] apply for the search warrant in court, the police will absolutely list out all the computer items that may be helpful to the police investigation, including the computer hard-disk, floppy disk, computer leads and monitor and explain to the judge why we may take away these items from the suspect's premises*."[289]

An online banking manager of a global bank based in Hong Kong interviewed for this research commented:

> "*I think that generally it is… probably takes slightly longer to piece together everything you need for computer crime, for online frauds. We, you know, work with the police to help us piece together stuff and work with our customers as well, if they find out that they've been a victim of any unauthorised transactions.*"[290]

Because the police in Hong Kong are trained to deal with computer related crime, they should be confident when explaining to a judge what they are looking for when they are applying for a search warrant. For example, in an interview for this thesis, a senior specialist computer crime prosecutor for the Department of Justice observed, "*I think [the officers from the Technology Crime Division] in my view are very professional, it's not ad hoc. They do know their way. They do it very professionally*".[291]

[289] Transcript 5 (HK) (In Chinese): p.1.
[290] Transcript 3 (HK): p.4.
[291] Transcript 2 (HK): p. 7.

This should means that the police already know what they are looking for and where the evidence is located, officers can quickly move to seize a suspect computer during the initial stage of an investigation. If there is a prima facie case for further investigation, the case will be investigated by the specialist Technology Crime Division within the CCB.

The Commercial Crime Bureau (CCB)

The computer crime section to the Commercial Crime Bureau (CCB) plays an important role in the policing of computer-related economic crime. The CCB has a long history of dealing with specialist economic crime. As an indication of the success in professionalising the police, the CCB is often regarded as a leader in fighting economic crime in Asia.[292] For example, in 2006 the CCB joined forces with the commercial crime unit of the Department of Justice and the South Wales Police in the UK, to arrest and charge seven people for possessing counterfeit credit cards. In the same year, the CCB pursued a fugitive in the US and had him extradited to Hong Kong. The fugitive was convicted in the High Court for fraudulently trading stocks and shares (amounting to HK$48 million) in 1982.[293] In 2005, a chairman and CEO of a publicly listed company was convicted on two counts of false accounting involving HK$300 million, and sentenced to six years' imprisonment. This complex case was regarded as a landmark case in Hong Kong because the fraudster was wealthy, sophisticated and well-connected in Hong Kong society. As the chairman of a listed firm, he could use his influence to hide or distort the evidence, making it difficult for the police to gather the evidence

[292] This was partly a result of a government push in the 1970s to establish various police-public partnership initiatives, such as the Fight Crime Committee, 17 District Fight Crime Committees and 1,200 Mutual Aid Committees. By the time the CCB was formed, fighting economic crime had become a high priority.

[293] See The Hong Kong Police Review 2006. [Online] [Cited 16/01/2009]. Available from: < http://www.police.gov.hk/review/2006/west/operations/04.htm>, p. 4.

needed to charge him. As the CCB stated, "*These cases illustrate the persistent determination of the Force [CCB] and its co-operation with the Department of Justice in bringing such complicated cases to trial*".[294]

Like the officers in the TCD, members of the CCB are professionally trained and expert in dealing with complex economic crimes, including overseas fraud. For example, in 1999, a senior inspector in the CCB was designated one of the top three international financial crime investigators at the investigator of the year awards in the United States.[295] Moreover, the evidence suggests that members of the CCB are willing to pursue fraud cases for lengthy periods of time, until they achieve some kind of closure.

The Independent Commission Against Corruption (ICAC)

The establishment of the ICAC in 1974 heralded a major turning point for Hong Kong. The ICAC was established as an independent anti-corruption organisation under two separate laws, the Independent Commission Against Corruption Ordinance (Cap 204) and the Prevention of Bribery Ordinance (Cap 201). Prior to the establishment of the commission, there was a deep seated belief amongst the public that corruption went to the core of the government. Setting up a new independent body was the only way the government could convince the public that it was serious about fighting corruption. In 2000, a third law, the Elections (Corrupt and Illegal Conduct) Ordinance (Cap 554) was introduced, extending

[294] See The Hong Kong Police Review 2004. [Online] [Cited 16/01/2009]. Available from: <http://www.police.gov.hk/review/2004/english/moperation.htm>.
[295] Lee, S. (October 27, 1999) 'SAR law duo win top US crime awards'. Hong Kong: South China Morning Post, p.6. Senior Inspector Cheung of the CCB, together with the chief investigator of the ICAC, smashed a hi-tech fake credit card production line in 1996. The forgers set up a computer data-base containing 40,000 account numbers to produce fake cards used to buy goods worth $44 million and had the potential to cause losses of about $280 million around the globe.

the remit of the ICAC as the guardian of public elections to ensure that such elections are conducted fairly, openly, honestly and free from any corruption.

According to Jones and Vagg, the ICAC uses a three pronged strategy to reduce corruption. Manion describes this as: a) enforcement to investigate and prosecute corruption; b) education to mobilise ordinary citizens to report corruption and increase the psychological costs of corrupt activities; and c) institutional design to reduce the opportunities for corruption in organisations.[296] The operations department is the law enforcement arm of the ICAC[297] and is the largest department, with 897 staff, representing 75 per cent of the Commission's total personnel. It is headed by the Deputy Commissioner, who is assisted by two directors of investigation, one responsible for the public sector and other the private sector. Overall, the department has three main responsibilities:[298] receiving, considering (filtering or vetting complaints) and investigating complaints. The operations department's powers to investigate are provided by the Prevention of Bribery Ordinance, 2) the Independent Commission Against Corruption Ordinance, and the Elections (corrupt and illegal conduct) Ordinances. Investigating officers have the power to arrest without warrant for offences stipulated in these three ordinances. It has essentially three responsibilities[299]: receiving and considering the complaint (filter or vetting of complaints) and investigating the complaint. Moreover, the investigating officers have the power to arrest without warrant for offences stipulated in the above three Ordinances. However, the investigating officers do not have direct access rights

[296] Jones and Vagg, (2007) Op Cit.: pp. 442-443.
[297] Independent Commission Against Corruption, (2006) Op Cit.: p. 34.
[298] Independent Commission Against Corruption, (2006) Ibid.
[299] Independent Commission Against Corruption, (2006) Ibid.

for entry and document seizure, but they do have the power to obtain court warrants to do so.[300]

The ICAC is a powerful anti-corruption agency and is directly answerable only to the Chief Executive (formally the Governor) of Hong Kong. An ICAC motto[301] states, "*Carry out our duties without fear or favour, prejudice or ill will*". As Miners[302] has explained, the ICAC occupies a unique position in the structure of the Hong Kong government. Moreover, under section 13 of the Prevention of Bribery Ordinance (Cap 201)[303] the commissioner of the ICAC has the power to investigate any person who is suspected of corruption. The commissioner alone

---

[300] Independent Commission Against Corruption, (2006) Ibid.
[301] Independent Commission Against Corruption, (2006) Annual Report 2006, preface.
[302] Miners, N. (1991) The Government and Politics of Hong Kong, (Fifth Ed.). Hong Kong: Oxford University Press, p. 95.
[303] "*(1) Where the Commissioner is satisfied that there is reasonable cause to believe-*
*(a) that an offence under this Ordinance may have been committed by any person; and*
*(b) that any share account, purchase account, club account, subscription account, investment account, trust account, mutual or trust fund account, expense account, bank account or other account of whatsoever kind or description, and any banker's books, company books, documents or other article of or relating to any person named or otherwise identified in writing by the Commissioner are likely to be relevant for the purposes of an investigation of such offence, he may for those purposes authorize in writing any investigating officer on production by him of the authorization if so required-*
*(i) to investigate and inspect such accounts, books or documents or other article of or relating to the person named or otherwise identified by the Commissioner;*
*(ii) to require from any person the production of such accounts, books, documents, or other article of or relating to the person named or otherwise identified by the Commissioner which may be required for the purposes of such investigation and the disclosure of all or any information relating thereto, and to take copies of such accounts, books or documents or of any relevant entry therein and photographs of any other article.*
*(1A) The Commissioner shall not, without the leave of the Court of First Instance obtain an ex parte application in chambers, issue an authorization under or by virtue of which any particular person who is alleged or suspected to have committed an offence under this Ordinance can be required to comply with any requirement of the description mentioned in subsection (1) (i) and (ii).*
*(1B) The Court of First Instance shall not grant leave for the issue of an authorization under subsection (1)(i) and (ii) unless, on consideration of an application under subsection (1A), it is satisfied as to the matters that the Commissioner is required to be satisfied under subsection (1).*
*(2) (a) Every authorization given under subsection (1) shall be deemed also to authorize the investigating officer to require from any person information as to whether or not at any bank, company or other place there is any account, book, document or other article liable to investigation, inspection or production under such authorization.*
*(b) A requirement under paragraph (a) shall be made in writing and any statement therein as to the existence of the appropriate authorization under subsection (1) shall be accepted as true without further proof of the fact.*"

can order an investigation under section 13 if there are reasonable grounds to suspect that a person is committing a corruption-related offence. Even without a court search warrant, ICAC officers can search and seize any documents located at any premises in Hong Kong, including bank account details. As Lo et al say,

> "*The powers enjoyed by the ICAC are considerably greater than those of the police. Its officers had the powers to search any premises without a court warrant, and to detain anyone on the premises for up to three hours. They could seize a suspect's passport for up to nine months with a magistrate court order even before a prima facie case had been established. They could examine bank accounts where it appeared that an offence might have been committed. They also had the power to forbid the mass media to disclose the identities of suspects before laying charges on them.*"[304]

These draconian search and seizure powers have attracted criticism from many quarters, including human rights activists[305].

Despite these criticisms, the ICAC plays a major role in protecting Hong Kong's international reputation as a financial centre. As InvestHK has stated, "*Hong Kong is one of the most corruption-free economies in the world. Cronyism,*

[304] Lo,T.W. and Yu, R.C.C. (Spring 2000) 'Curbing Draconian Powers: The Effects on Hong Kong's Graft-Fighter'. International Journal of Human Rights, Vol 4 No.1. p.55.

[305] In recent years, the ICAC have been accused of infringing the freedom of the press, and some of these special search and seizure powers have been challenged in the courts. For example, on August 2004, the South China Morning Post reported that the ICAC made ex parte application for 14 special search warrants in the Court of First Instance and the court granted those warrants. In July 2004, the ICAC armed with these search warrants, raided the offices of seven newspapers to investigate a leak that caused the identity of a woman allegedly assisting the ICAC in a fraud case to be revealed, an offence under the Witness Protection Ordinance. After the raids were made, there was a public outcry, because the public have a strong feeling that the ICAC has infringed the freedom of the press. The newspapers challenged the search order by seeking a judicial review in the Court of First Instance. The court ruled the ICAC was wrong and the judge ordered the search warrants to be set aside and the seized material returned to the newspaper companies respectively. As Justice Hartmann said "The ICAC should not have automatically resorted to a draconian law, when it could equally have achieved its legitimate aim by less intrusive measures such as a production order requesting assistance from newspapers. The powers granted to the ICAC had to be viewed through the prism of Article 27 of the Basic Law, which protects press freedom." See Shamdasani, R. Wong, M. (Wednesday, August 11, 2004) 'ICAC was wrong over news raids, court rules'. Hong Kong: South China Morning Post, p.1.

*influence-peddling and bribery receive zero tolerance here".*[306] Transparency International, which compiles annual data and statistics on corruption, has consistently ranked Hong Kong among the places that are the most free of corruption. [307] The ICAC is also a model for the rest of Asia.[308]

Reflecting its proactive strategy, the ICAC recently identified the Internet and the financial sector as two areas where corruption is growing. In 1999, the ICAC established a computer forensics section to support its frontline investigators in dealing with computer crimes, including Internet fraud. The computer forensics section works closely with the police and other law enforcement agencies, especially the TCD, to keep abreast of the trends in computer crime. It is not unusual to find the ICAC and the police mounting joint operations to raid high profile targets.

The establishment of the Financial Investigation Section within the ICAC has improved investigation of complex corruption related financial fraud, as suggested by the ICAC Annual Report:

---

[306] The InvestHK, [Online] [Cited10/06/2008]. Available from: <http://www.investhk.gov.hk/pages/1/160.html>.

[307] For example, in 2007 the Transparency International Global Corruption Barometer ranked the Hong Kong government as among the most effective in fighting corruption in world. In 2008, the Transparency International's Corruption Perceptions Index also ranked Hong Kong as the 12th least corrupt place in the world (the UK was ranked 16, the United States 18 and Germany 14). See The Transparency International, (6 December 2007) 'Report on the Transparency International Global Corruption Barometer 2007'. Berlin: Policy and Research Department. p.13.

[308] Transparency International, CPI_2008_table. [Online] [Cited 17/01/2009]. Available from <http://www.transparency.org/news_room/in_focus/2008/cpi2008/cpi_2008_table>. In April 2008, when Malaysia proposed to restructure its anti-corruption agency, the Malaysian government recommended restructuring along similar lines to the ICAC in Hong Kong. See New Sabah Times, (April 2008) 'PM Studying Proposal to remodel ACA'. KK: Malaysia, p. Home 8. A minster in the Prime Minister's Department, Datuk Seri Mohamed Nazri Abdul Aziz, stated: "*the ACA had suggested following operating style of the ICAC, since inception, the ICAC had embraced a three-pronged approach of law enforcement, prevention and community education to fight corruption. With the support of the government and the community, Hong Kong has now become one of the "cleanest" places in the world*".

> "*The service of forensic accountants within the Financial Investigation Section (FIS) has increased steadily, following an increase in the number of complex corruption related fraud cases investigated in 2007. Investigations conducted by FIS registered a notable increase of 23% from 150 cases in 2006 to 185 cases in 2007, with an aggregated sum of HK$4.91billion.*"[309]

The ICAC investigates all types of economic crime, including Internet fraud, where the ICAC's special search and seizure powers can be useful. For example, if a fraud case is suspected to be related to corruption, the ICAC can use their special powers without going through the process of applying for a search warrant. This can save a lot of valuable time and prevent data from being erased. The ICAC can act fast and enter an offender's home or office to gather electronic evidence before he or she destroys the evidence or the electronic evidence disappears from the ISP's server. Moreover, the ICAC can also use its special powers to search and seize an offender's (and their associates') bank details inside the bank's computer system, without the suspect even realising it.

The ICAC also works closely with other law enforcement agencies, such as the police, in investigating economic crime. Even if an initial investigation finds that a case may not be corruption related, the ICAC can pass the case on to the TCD for further investigation. If the ICAC does pass the case on, the TCD must decide what approach to take next, in terms of gathering further evidence with a view to prosecuting the offender. Because the ICAC will have already gathered most of the evidence, the TCD has a relatively easy task in locating the evidence and the offender. In 2003, Ambrose Lee, the Commissioner of the ICAC,

[309] The ICAC, (2007) Annual Report 2007, p.48.

speaking at a workshop at the 11th International Anti-Corruption Conference held in Seoul, said that:

> "*The Operational Liaison Group has been set up for directorate officers of the Police and the ICAC to meet regularly on operational matters of mutual interest. Briefings on operational issues are also held regularly for different levels of the Police. These well-established channels allow the Police and the ICAC to join hands to combat corruption both from within and outside the police organisation... the Police are in fact our close ally in crime-fighting. We have exchanged information on cases of mutual interest and waged joint operations where appropriate. Together we have made Hong Kong a safe and corruption-free city to live in and to do business.*"[310]

As this shows, the ICAC works in a coherent manner with other law enforcement agencies, such as the police, in investigating economic crime, and will pass on economic crime cases to the police if they find the case is beyond their remit (See **Case 5** and **Case 14)**.

Unlike the HKMA, the ICAC has prosecution powers in financial fraud investigations. The ICAC also has wider powers than the police to fight financial crime, especially financial crime involving corruption. As Snell and Herndon[311] state, the ICAC can place considerable pressure on businesses in Hong Kong. The ICAC has the power to conduct overt and covert investigations[312] and to prosecute suspected cases of corruption (including financial fraud and IT crime) in the public and private sectors. The ICAC also conducts programmes to educate the public against the evils of corruption and to foster public support[313] (e.g.,

[310] Lee, A.S,K. (27/05/2003) 'Corruption in the police: How do you clean it up', Hong Kong: ICAC. [Online] [cited 26/01/2009] Available from: <http://www.icac.org.hk/en/services_and_resources/sa/cp/index.html>.
[311] Snell and Herndon, (2004) Op Cit.: p. 83.
[312] Independent Commission Against Corruption, (2006) Op Cit.: p. 16.
[313] Independent Commission Against Corruption, (2006) Op Cit.: pp. 74-75.

meet-the-public sessions, ICAC club and TV dramas). As Jones and Vagg state,[314] when the ICAC first introduced this kind of sophisticated media propaganda against crime in 1975, it was regarded as new to Hong Kong.

The ICAC's reputation in fighting corruption means that the victims of corruption also have confidence in it as an organisation. In its 2006 report,[315] the ICAC stated that of the 3,339 reports of corruption received during 2006, 2,440 were made by complainants who identified themselves, representing 73 per cent of the total reports received.

The corruption prevention department of the ICAC has as its main responsibility the task of minimising the opportunities for corruption in the existing practices and procedures of public departments and agencies, including the HKMA.[316] This is achieved mainly through examining and reviewing work procedures to weed-out any weaknesses that are conducive to corruption. The corruption department also works with other government agencies to identify corruption prone areas for review and to monitor the implementation of recommended corruption prevention measures. It can also be requested to provide free corruption prevention consultation services to private organisations, such as banks.

The community relations department is the educational arm of the ICAC. The second largest department with 162 staff,[317] the main goal of community relations is to educate and enlist public support against corruption under sections 12(g) and

[314] Jones, C. and Vagg, J. (2007) Op Cit.: p. 442.
[315] Independent Commission Against Corruption, (2006) Op Cit.: pp. 35-36.
[316] Independent Commission Against Corruption, (2006) Op Cit.: p. 49.
[317] Independent Commission Against Corruption, (2006) Op Cit.: p. 66.

(h) of the Independent Commission Against Corruption Ordinance.[318] Its duties are:

> *"To publicise anti-corruption messages and fortify community support through extensive preventive education programmes and special projects [e.g. TV series on detecting and prosecuting corruptions] targets at civil servants, young people, selected trades and professions in the business sector as well as candidates and agents participating in various elections. In parallel, the Department continued to heighten public awareness of the evils of corruption and the importance of maintaining Hong Kong's reputation as a clean and fair place in which to live and conduct businesses through various publicity programmes."*[319]

In 2006, 963 corruption prevention training seminars were conducted in various branches of the private sector, which were attended by a total of 8,823 managers and 30,732 frontline staff.[320] Moreover, in 2006, 75 per cent of the 767 publicly listed companies in Hong Kong invited the ICAC to formulate or review their staff code of conduct or to arrange ethics training for their employees.[321] The banks in Hong Kong are also encouraged to undertake these review and training programmes, which can effectively reduce the levels of fraud and corruption among bank employees and increase the likelihood of bank employees reporting any instances of crime to the authorities.

The Technology Crime Division (TCD)

The TCD plays a major role in policing Internet banking fraud in Hong Kong. A good overview of the TCD was given by a Superintendent of TCD interviewed for this research:

[318] Ibid.
[319] Ibid.
[320] Independent Commission Against Corruption, (2006) Op Cit.: p. 68.
[321] Independent Commission Against Corruption, (2006) Op Cit.: p. 69.

> "*Right, in general, the Hong Kong police have set up a particular specialised unit within the Commercial Crime Bureau. That particular division is known as the TCD, the Technology Crime Division, which is composed of 60 people headed by a Senior Superintendent. His deputy is me, the Superintendent of TCD. Under us are basically three sections. The first section is the Ops Section, headed by a Chief Inspector responsible for all types of investigation. The second section is what we call the computer forensics, and is mainly composed of the computer forensics lab, which examines and handles all the digital evidence. And the third section is the intelligence support section, that's the section which deals with local and overseas liaison, crime prevention, cyber-intelligence etc... And of course, also there is a small training unit, housed under the forensic unit, which is responsible for training. This is at the headquarter level we have these division set up. As regards the regions, in Hong Kong there are five land regions: Kowloon East; Kowloon West; Hong Kong Island; NT North and NT South. Each land region has their regional crime unit. Within the regional crime unit, we also set up a small team which is known as the TCU, the Technology Crime Unit, which is headed by a senior inspector. They are responsible for the work in the regions. Of course, they have just been set up for about few months, and what we are planning to do is try to expand the cyber-crime investigation capability to the regions and districts. That, in general, gives you a really broad picture about how the Hong Kong police are dealing with Internet related crime.*"[322]

When the TCD's computer crime section was first established in 1993, only a few computer related crimes had been reported to the police. For example, in that year, only four cases of computer crime were reported (three involving fraud or theft and one involving hacking). However, two years later, in 1995, 14 cases of computer related crime were reported to the police (four cases of hacking, eight of fraud and two of criminal damage). In the same year, the police cracked a sophisticated cross-border credit card fraud ring involving gangs in Hong Kong and Shenzhen City. The offenders sold fake credit cards accounts for US$250.

[322] Transcript 4 (HK): p.1.

Members of the TCD seized the ring's computer equipment and credit data.[323] In another case in 1996, Wong says "*a disgruntled computer technician brought down a network by hacking into the Reuters trading network in Hong Kong*"[324] This crime shocked the authorities. The police responded by upgrading their computer crime section to a computer crime unit and increasing police personnel in the new unit. An academic also openly attacked some judges in Hong Kong as lacking computer literacy:-

> "*Some judges don't even know how to send an e-mail, lack of computer knowledge means judges cannot understand computer and digital evidence easily. This would hamper efforts to secure a successful prosecution because it's the prosecutor's responsibility to prove the effectiveness of evidence.*"[325]

In 2000, there was a surge in the number of computer related crimes in Hong Kong, with 368 cases being reported to the police that year (238 involved hacking, 49 were Internet fraud or theft cases, 29 involved online deception and 15 were criminal damage cases).[326] This provoked a comprehensive response from the authorities.

In April 2000, the courts put the first computer hacker behind bars.[327] A police spokesman warned:

---

[323] Wong, K. (2005) Op Cit.: p. 28.
[324] Wong, K. (2005) Ibid.
[325] Tse, S. (2000, 01-18) 'Judges must log into the Net Crimes'. Hong Kong: Hong Kong Standard, p.A03.
[326] Lau, L.Y.C. (2005) Ibid.
[327] A 19 years old teenager, Po Yiu-Ming was jailed at Eastern Magistracy for hacking into computers to obtain account details and passwords and selling them for profit (theft). This was the first case brought to court involving an internet user selling stolen data to reap unlawful profits. The Magistrate, Ian Candy, said in sentencing Po that the impact of computer hacking crimes was enormous because the internet was widely available and used. The offences were serious and had to be dealt with by deterrent custodial sentences. See Chu, Y.C. (2000, 04-06) 'Net hackers put behind bars in SAR First' Hong Kong Standard, p. A03.

> "*The havoc caused by hackers was a great concern in Hong Kong regarding the reliability and trust in conducting e-business on the Internet, stressing that police would continue to take stringent enforcement actions* on *e-crime offenders."* [328]

As Senior Superintendent Ng Kam-Wing of the TCD said at the time, *"People are no longer breaking into other people's computers for fun. They are committing crimes in various information technology media."* [329]

In response, the police established a police task force comprising specially trained officers to crack down on such crimes. Eighty officers, some of whom were trained overseas, were temporarily seconded from other police departments. The Police Commissioner also said that:

> *"The Security Bureau might amend existing legislation to expand the powers of police in investigating computer offences. The University of Science and Technology is designing a programme on computer forensic science to help police and other government departments gather criminal evidence*." [330]

The government announced a fight against computer crime. As Poon says,

> *"The [Government] has established an inter-departmental working group which consisted of Information Technology and Broadcasting Bureau, the Department of Justice (DoJ), the police and the ICAC to crack down on illegal activities on the Internet and co-operate with Interpol, the FBI and Royal Canadian Mounted Police to review existing law.*" [331]

In 2000, a specialist computer crime prosecution unity was also established in the Department of Justice. The government also announced that it would be stepping

[328] ISD, (2000, 12-14), Hong Kong Government, Press Release.
[329] Ng, M. (2001,08-8) 'Five-fold rise in computer crimes', Hong Kong: HKIMail, p.A06.
[330] Moy, P. (2000, 01-7) 'Computer crime the big challenge for police'. Hong Kong: Hong Kong Standard, p.A03.
[331] Poon, D. (2000, 01-23) 'Inter-agency war on net crime'. Hong Kong: Hong Kong Standard, p.A03.

up the fight against computer crime. Since then, the police and other agencies in Hong Kong have kept a close eye on computer related crime. There are a number of reasons for this. First, computer related crime can be very profitable for organised gangs in Hong Kong and southern East Asia.

Second, if this type of crime did flourish in Hong Kong, it could threaten Hong Kong's reputation as a financial centre. As a Superintendent from the TCD interviewed for this research stated:

> "*One of our [policing] priorities is cash crime, because Hong Kong is an international hub, so a lot of people are engaged in quick cash crime, or may be sometimes street deception etc. So, we want to deal with it"* [332]

In effect, the government and the police declared zero tolerance on illegal Internet activities. The birth of the Technology Crime Division was announced on September 2001. It consisted of 42 police officers. According to the government press release:

> "*35 of these police officers have attained tertiary qualifications ranging from bachelor to doctorate degrees in computer science or related fields and another 31 suitably qualified officers will be joining the TCD over the next two years.*"[333]

Integrity of Evidence

Because of their high level of expertise, the Hong Kong police are likely to be successful in their applications for search warrants and to conduct effective searches. If a case is passed on by the Technology Crime Initial Response Cadre (TCIRC) from a local police station, it is likely to be looked at immediately and a search warrant served very quickly by the officers from the TCD, because the

[332] Transcript 4 (HK): p.16.
[333] ISD, (2001, 09-12) 'Targeting Techno crime' Hong Kong Government, Press Release.

TCIRC and the TCD communicate directly with each other. Moreover, as the TCD is the only police division that deals specifically with technology related crimes, the case is likely to be immediately investigated by specialist police. A Superintendent from the TCD interviewed for this research explained that:

> "*Basically we are concerned about the data integrity of digital evidence. So when an officer attends the scene of crime, there is a set of special procedures and guidelines they have to follow so that they know how to pack the exhibit, and send it back to our lab for examination. If they require some sort of examination at the scene of the crime, then they will call out our computer forensic examiner. Then our computer forensic examiner will turn out to the scene and conduct the examination.*"[334]

A Sergeant from the TCD interviewed for this research also pointed out that:

> "*When we established the TCD, we had a forensic team and a forensic lab. We are all trained and already have extensive experience on computing. Each one of us will be specialised within a certain area in computer science, because we have already attained a certain level academically, as well as reached a certain standard in IT skills. As a result, we have no problem using sophisticated computer forensic tools [at the scene of crime], such as EnCase, to help us to keep and retrieve the computer evidence. The way we handle the electronic evidence and collect the evidence, is in accordance with international recognised procedures. As a result, we can document each item and log each step. So far we never have had any problem with admissibility in court, because we are all aware that the real test of the electronic evidence is in the court.*"[335]

Knowing how to collect and preserve evidence is essential to its admissibility in court. TCD officers are often professionally trained before they join the police. Furthermore, all officers are university graduates with a certain level of expertise in IT and most have prior work experience in IT. Therefore, officers in the TCD

[334] Transcript 4 (HK): p.2.
[335] Transcript 6 (HK) (In Chinese): p.1.

tend to be proficient in preserving and maintaining the integrity of electronic evidence.

Effectiveness

Given the existence of these specialist computer crime units, it is reasonable to expect that a high proportion of reported cases of fraud will end up as recorded crimes and successful prosecutions. However, as Table 7.1 shows, the police do not always record all reported cases of fraud as crimes. For instance, on average, only 30.72 per cent of the cases of fraud reported between 2002 and 2007 were recorded as crimes. However, over the same period, on average, 87.75 per cent of the cases of business fraud reported to the police were recorded as crimes. As these figures suggest, the police are more likely to record a reported case of fraud as a crime when the victim is a business. Therefore, business fraud seems to be treated more seriously than other types of fraud in Hong Kong.

As aforementioned, a number of the businesses (especially the banks) in Hong Kong routinely work with the CCB to prevent fraud. As a result of this co-operation, trust has been established between the police and the businesses. When reporting fraud to the police, these businesses will most likely report directly to the CCB instead of reporting the incident at a police station. As a result, cases of business fraud are directly recorded and investigated by officers in the CCB. These officers are specially trained to handle business; some even qualified in accountancy. Therefore, the officers are immediately able to establish whether or not fraud *has* been committed, what evidence is needed and how to proceed with

the investigation. These factors help explain why the recording and detection rates for business fraud are high.

**Table 7.1: (All Policing Districts) Hong Kong Police Fraud Statistics: Attrition Rate between Reported and Recorded Fraud (Deception and Business Fraud))**

| Fraud Off. | Reported 2002 | recorded & detected: 2002 | reported: 2003 | recorded & detected: 2003 | reported: 2004 | recorded & detected: 2004 | reported: 2005 | recorded & detected: 2005 | reported:2006 | recorded & detcted:2006 | reported:2007 | recorded & Detcted:2007 | Diff. in% Between Reported & Recorded & detected (Total Average.) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Decep.** | 4656 | 1208 | 4732 | 1168 | 4009 | 1025 | 4076 | 984 | 4758 | 1137 | 4745 | 1359 | 25.51% |
| **Bus. Fraud** | 52 | 44 | 33 | 28 | 20 | 16 | 19 | 18 | 34 | 31 | 27 | 25 | 87.57% |
| **Total** | 4708 | 1252 | 4765 | 1196 | 4029 | 1041 | 4095 | 1002 | 4792 | 1168 | 4772 | 1384 | 30.72% |

*(Sources: Hong Kong Police: Crime Figures 2002, 2003, 2004, 2005, 2006, 2007; Annual review 2002/2003, 2003/2004, 2004/2005, 2005/2006, 2006/2007)*

Table 7.2 shows the statistics for reported technology related crime in Hong Kong from 2003 to 2007, including online banking theft. The figures for online banking theft can be seen to vary, with eight cases reported to the police in 2003, 19 in 2004, three in 2005, none in 2006, and only one in 2007. This reached a peak in 2004, then dropped again in 2005. These fluctuations in the reporting of online banking fraud may be related to periodic increases in the police investigation of Internet banking fraud (in 2004, three people were convicted and two sentenced to up to 4 years imprisonment for Internet banking fraud[336]).

However, it is unclear how many cases of online banking theft were actually *recorded* as crimes by the police because these data are not publicly available. Nonetheless, Table 7.2 does confirm that the police keep internal records of

[336]Lin, S. (2004) Review of Scams and Related Crimes in 2004, Technology Crime Division, Hong Kong: Hong Kong Police. [Online] [Cited 24/11/2008]. Available from: <http://www.hkcert.org/ppt/event111/phishing1_hkpf.pdf>, p. 15.

specific technology related crimes, which further indicates that the police have a policy of keeping a close eye on technology crime.

**Table 7.2: Technology Related Crime Statistics in Hong Kong (Reported)**

| Offence | 2003 | 2004 | 2005 | 2006 | 2007 |
|---|---|---|---|---|---|
| **Unauthorized access to computer by telecommunication** | 47 | 11 | 8 | 6 | 6 |
| **Access to computer with criminal dishonest intent** | 356 | 329 | 441 | 471 | 333 |
| **Criminal damage** | 16 | 11 | 6 | 5 | 4 |
| **Obtaining property by deception** | 86 | 105 | 145 | 193 | 215 |
| **Obtaining services by deception** | 17 | 15 | 9 | 12 | 8 |
| **Thefts (Online banking related)** | 8 | 19 | 3 | 0 | 1 |
| **Others (criminal intimidation, using a false instrument etc.)** | 58 | 70 | 41 | 54 | 67 |
| **Total** | 588 | 560 | 653 | 741 | 634 |

*(Source: Technology Crime Division, Hong Kong Police. [Online] [Cited 05/11/2008]. Available from Internet: <http://www.police.gov.hk/hkp-home/english/tcd/overview.htm>)*

One explanation for the apparent increased willingness to report cases of online banking fraud to the police relates to increasing public awareness of Internet banking fraud. The HKMA, the police and other agencies have organised anti-Internet banking fraud campaigns through various channels, including educational leaflets, television and radio programmes, and an interactive computer programme on Internet banking security.[337]

Summary

The Hong Kong police have been able to increase their capabilities in fighting computer related crime in a relatively short period principally because this kind of crime has become a government priority. As a result, the government has invested increased resources in police recruitment, training and organisation in

[337] Hong Kong Year Book (2004) 'Banking Sector'. Hong Kong: Hong Kong Government. [Online] [Cited 24/11/2008]. Available from: <http://www.yearbook.gov.hk/2004/en/04_03.htm>.

this area. However, despite the existence of the various specialist computer crime agencies, it remains unclear whether *reported* Internet banking fraud is in fact more likely to be *recorded* as Internet-related crime. Nor is it clear whether this also means that cases of Internet banking fraud will be prosecuted as Internet related crimes.

# Chapter Eight
# Police Strategy, Training and Recruitment

## Introduction

In the previous chapter, I suggested that the Hong Kong police have deliberately increased their capability in relation to Internet crimes such as Internet banking fraud, partly because the government wishes to protect Hong Kong's economic environment and its international reputation as a financial centre. In 2011, a Hong Kong Stock Exchange's press release revealed organised attack on the HKExnews Website and a disruption of service, exactly the kind of event the government and business wishes to avoid. The press release said:

> "*Since the interruption, HKEx's Information Technology team has been working closely with local and overseas security experts to investigate the cause of the attack and restore normal service…Engineers are on site today at HKEx's data centres to provide necessary support for the stable operation of the HKExnews website. HKEx is also in close cooperation with the Technology Crime Division of the Hong Kong police.*" [338]

In the 1990s, following the adoption of the 'zero-tolerance' approach to Internet crimes, a series of strategies were implemented which resulted in the establishment of the TCD. Today, the TCD are confident and positive about their capacity to fight technology related crimes, and compare themselves to the best in the world. According to the head of the TCD, the TCD is currently benchmarked against the FBI, the world's most renowned computer crime investigative agency:

> "*We still strive here in HK to increase our law enforcement capability in comparison with other agencies. The way I look at it, they may not be better than us, but different agencies got different strength and weakness. We put FBI at the top, then the National Hi-*

[338] See Hong Kong Stock Exchange (11/08/2011) <http://www.hkex.com.hk/eng/newsconsul/hkexnews/2011/1108112news.htm>, visited 22/6/2013 .

> *tech Crime Unit in the UK [this Unit was dissolved by the UK government in April 2006]. We are between them, in some areas we are parallel.*"[339]

The TCD's push to be amongst the best in the world has led to the adoption of a policy of regularly upgrading police capability in this field. Referring to a Police Commissioner's address to the force in the 1990s, a Chief Inspector from the TCD interviewed for this research said:

> *"The Commissioner of the Police, in his policy address, said that we must establish the capability and also that he would put resources into it. The organization as a whole knows we have to learn about computer crime. Of course, there are number of challenges. The developments of a technology capability in the police need lots of money, against the budget restraints. The investment in the technology crime capability will never stop but only grow. This is unlike the traditional crime enforcement capability, i.e. revolvers for uniform [ranks] or detectives that have usually been there for years. They may change to a new barrel, but it will last for about ten years. Like us with the computer software and hardware - everything involved in the investigation of computer related crime - new technology keeps coming up. If you don't use it, the criminal out there will use it. Not to mention the organized crime groups. They have the financial capability to do it. And training also takes up time too. So, it is not the sort of investment that you can just put in then suspend for a number of years… I can tell you, last year our budget in our division (we are one of the 5 divisions in our bureau, and our bureau is within 5 or 6 division in the Crime Headquarter) our division budget alone is greater than all the bureaux and sometimes it is very difficult to explain to other divisions within the police force, who are also in need of money to expand or maintain their services, that TCD needs that sort of money. We only look at 200 odd computer crimes in a year. It is a dilemma that the Commissioner is facing. Then, as an organization as a whole, equipping the officers with IT knowledge and investment on the capability on the IT crime is a necessity."* [340]

[339] Transcript 7 (HK): p.13.
[340] Transcript 8 (HK): pp.7-8.

This investment in capability is associated with the TCD's overall strategic plan, and recruitment and training initiatives.

i) Strategy

The head of the TCD interviewed for this research outlined the strategic approach taken by the police in the following terms:

> *"The Hong Kong police take the eight points approach in tackling technology crime, or computer related crime. By rendering these eight point strategies, we are hoping to form and establish comprehensive enforcement strategies, architectural and directive, in tackling technology crime problems. The eight point enforcement strategies consist of the following points: maintaining a professional investigation capability (i.e. how we train up our men, sustain the expertise on computer related crimes); fostering the computer investigation capability throughout the force (i.e. how we pass the skills downward from the divisional to the district frontline officers, on how to handle technology crime. Through this way we have set up the Technology Crime Division in this Headquarter. We have set up a different technology crime unit around Hong Kong. At the same, we have recruited an initial response technology crime cadre. They will be trained and pass on computer crime knowledge. Then they will act as the auxiliary to the computer crime expert in the Headquarters, as frontline officer).*
>
> *Thirdly, we've developed our accredited computer forensic capability. That is to say we are recruiting outside experts to work with us on the computer forensics, and we train our own men in forensics, together with the University of Science Technology of Hong Kong [UST] to form a training school, which is an accredited training course, then send our men there. At the same time, based on the syllabus from the UST, we have revised our own training strategies, and then we started two levels of training with the force. Therefore, there are three levels of training. The highest one is at the University, then the other two are from the force, but those who attended the University course would qualify as computer forensic examiners. In court they will be treated as expert witnesses. When they give evidence in court, it would be accepted by the court…*

*The fourth one, we will constantly review our law, to make sure our law covers the situation.*

*Then the fifth one, we also form a crime prevention Unit to form different strategies and series of prevention programmes… this term crime prevention in fact can be separated. It can be part of the law enforcement strategies. Police technique cannot just concentrate all the effort on arrest and prosecution, but on the other hand need to let the public know about what the crime is all about, in order to prevent or avoid it happening again. So, it is part of the whole tackling technology crime strategy. Theoretically it is effective, right, to tell people not to fall into the trap, but practically, very much depends on the timing, on the target group. If we separate them into a separate target, tackling it at school, primary school, secondary school, then the university. You target it at higher secondary or those drop-outs separately. So, overall it is part of our enforcement strategy. We think that what we are doing is quite successful. We are targeting the young at primary school, some at secondary and early youth, some in businesses organisations and some of the general public. So, the crime prevention programmes are commencing and are separate from the technology division. So we have to wait and see. We only commenced this programmes about nine months… [ago]…*

*The sixth strategy is the intelligence management and the issues relating to industry and professionals. We think that the effect of the police and the law enforcement alone, the chances of success or the effectiveness of the enforcement, will not be that good, because the industry and professionals, they have the technology and the new products. Without the industry and professional's help, it will be a challenge for us.*

*The Seventh strategy is the collaboration between the global and the local law enforcement agencies. To put it this way, in Hong Kong we have four major law enforcement agencies who are carrying out computer related and technology crime enforcement. The Immigration agencies for immigration-related tasks, the Customs and Excise for copyright, and the ICAC for corruption offences. The police force is the additional one, carrying out the task. So, every six months, we have to get together for a management meeting among these agencies, to talk about strategies, thinking and basically to share working experience. We've also got the overseas*

*visits. It is very active. We have been visited by many overseas agencies and we also visit overseas agencies. We also joined in partnership with them. Also conferences and seminars. I think all agencies around the world are doing the same. But we are in a better position than they are, because in Hong Kong, the police is the lead agency. So what we do, and what we promise we will do outside Hong Kong, other agencies in Hong Kong would simply follow, rather than just, say, represent just the police side. For example, in the USA, the police only represent a small part of the law enforcement, because of the fragmentation among the law enforcement agencies. In Hong Kong, the police is* ***the*** *key agency. Of course, our liaison work is quite good.*

*The last one, which is the magic sentence, we continue to improve and deliver the best practice, to keep you on track with the advancement of information technology, (i.e. we understand that the technologies are changing, a lot of new things are coming up). The tackling of the new technology crimes is a new area for everybody. Still there are a lot of things waiting to be explored. Different crime targets, different modus operandi. So, those are our enforcement strategies. By introducing different activities to support and enhance our capability to handle technology crime."* [341]

The TCD has a number of custom-made strategies for building the force's capability. In an interview for this thesis, a director of the forensic section of an international management consultancy, thought that the TCD had been successful in this regard, stating that, "*Perhaps there is not a [capability] issue for the Hong Kong Police. They have a lot of staff and technology to deal with this matter*".[342] In addition, the Hong Kong police have developed networks with local and overseas experts in the field. As the head of the TCD interviewed for this research stated:

"*At I has mentioned earlier, beside getting our officers to train, we are in fact forming strategic partnerships with different parts of the world, but locally first, we form a partnership with HKU. Every year we have a high*

[341] Transcript 7 (HK): pp.1-3.
[342] Transcript 1 (HK): p. 6.

*level meeting, that was including myself, then do a network meeting to talk about what were the problems, whenever we need their services or assistant they would be there.*"[343]

ii) Training

Police training needs to be thorough and ongoing because new technologies keep appearing on the market. As a Superintendent from the TCD interviewed for this research said:

> "*We set up this particular specialised [TCD] division within the force to handle all these matters, you know. We have our training strategy to train up our officers here. We provide a lot of seminars and talks. We are doing that for the general public to increase public awareness, so that they'll be less cheated over the Internet. We do have an education programme with the education department for the high-school and the primary school kids. We have special talks for IT [industries], for lawyers, for the IT security professions. We also have a lot of seminars for the prosecutors, for the judges. So [we can] improve their awareness and make them understand all the basic terminology of the computer and the Internet. So this would help us a lot. I think crime prevention is one of the very important strategies to tackle all these issues. As regards the public, at the end of the day, right, for all the fraud cases, I think greed is the first important issue. So, we have a web-site set up to give a lot of information to the public, so that they'll be aware of that, not to fall into the play of those criminals. These are the ways we have tackled the problem. Finally, we team up with the University and together come up with formal training for our officers, not just their practical knowledge. Because IT changes rapidly, we want to improve the concepts, the [theories] themes and understanding the principles of IT or computers. Hopefully, the training they gain will have a longer effect.*"[344]

As another Chief Inspector from the TCD interviewed for this research explained:

> "*When you talk about computer crime, it is a totally different story, that you never stop learning, because development of the computer technology and the Internet,*

[343] Transcript 7 (HK): P.5.
[344] Transcript 4 (HK): pp.6-7.

> *it is unlike the traditional crime investigator. The things you learnt 20 years, you still can apply the knowledge to-day, but with the computer, 20 years time is totally different. So you have to keep learning. You may be a good computer crime investigator to-day, but in two years' time, you will be outdated*."[345]

The push for continuous training was confirmed by a sergeant from the TCD in an interview for this thesis, who said that, "*We are continuously kept on training, because within the police there is regular training on computing*".[346] Similarly, a police officer from the TCD interviewed for this research argued that:

> "*Yes, there is opportunity for training, but sometimes there is a limit to the seats available, so we also supplement with the learning ourselves, by going to outside courses, one cannot rely on the TCD to provide all the training.*" [347]

(iii) Police Recruitment

The police have a two-tier system for recruiting officers: a stream for inspectorate grade officers and another for police constables. Applicants can directly apply for the position of police constable or police inspector. Each stream has specific formal academic requirements for each. For example, the police inspector applicants require language skills, while there are minimum educational requirements to become a police constable.[348] For a police constable, the minimum education requirement is as follows:

> "*Applicants must reach minimum educational attainment of Secondary School Form 5 and they must have obtained a pass or above or equivalent either in five subjects, including Chinese Language and English Language*

[345] Transcript 8 (HK): p.7.
[346] Transcript 6 (HK) (In Chinese): p. 2.
[347] Transcript 5 (HK) (In Chinese): p.8.
[348] Applicants must possess level 2 or above Chinese Language and English Language in the HKCEE or equivalent. If applicants do not meet these requirements they can still apply if they pass the Chinese and English papers in the written examination during the selection process.

> *(Syllabus B before 2007), at level 2 (or Grade E before 2007) in the Hong Kong Certificate of Education Examination (HKCEE); or three subjects, including Chinese Language and English Language (Syllabus B before 2007), at level 2 (or Grade E before 2007) in the HKCEE."* [349]

For Police Inspector, the applicants must either:-

> *"possess a Hong Kong Degree or equivalent, or an accredited Associate Degree from Hong Kong tertiary institution /a Higher Diploma from a Hong Kong polytechnic / polytechnic university, or a Diploma from a registered post-secondary college awarded after the date of its registration, or equivalent; or a pass in two subjects at Advanced Level in the Hong Kong Advanced Level Examination (2A) plus three other subjects at grade C or above in the HKCEE (3 O), or equivalent."* [350]

Overall, the police regard formal education as an important requirement. As Jiao says,

> "*The police job has become very competitive in Hong Kong, because there is a large pool of qualified applicants. Although police constables can be admitted into the police with HKCEE, police inspectors must have a University Degree*."[351]

The selection process for police applicants is strict and the entry thresholds are high, as the police want to attract high calibre applicants. One way of attracting high calibre applicants is to remunerate them well. The remuneration for an inspector with a university degree is high, starting at between HK$29,715 and HK$56,335 per month, plus housing allowances

[349] See Hong Kong Police. [Online] [Cited 15/05/2008]. Available from: < http://www.police.gov.hk/hkp-home/english/recruitment/entry.htm#Constable>.
[350] See Hong Kong Police [Online] [Cited 15/05/2008]. Available from: < http://www.police.gov.hk/hkp-home/english/recruitment/entry.htm#Inspector>.
[351] Jiao, A.Y. (2007) Op Cit.: p.81.

and other government subsidies.[352] In Hong Kong, a police inspector occupies a highly respected position in society. As Jiao states, "*The official theme of recruitment for them is "to be a leader". Inspectors, as a matter of fact, are depicted as the elite of Hong Kong society during the recruitment process".*[353]

The police also directly recruit large numbers of highly educated police inspectors who have already attained computer science or other science-related degrees. Some of these recruits are selected to take up specialist training and become computer crime investigators. Overall, as the head of the TCD interviewed for this research outlined:

> "*In 1999, before we built up our enforcement structure, we started with Hong Kong University of Science and Technology to set up a training programme to be completed by the police officer as the computer forensic examiner, so that they can assist the investigation with computer crime. That is how we look at it, as our top priority. At the time, when we first started the programme with the HKUST, we only got 17 police officers. Now we've got 60 odd police officers. The programme between the years 2000-01 has been upgraded to postgraduate diploma. We do not employ outside experts, because we scan from 20,000 [police] officers in the force, those with good education, with a University degree, a PhD. and a computer-related degree.*"[354]

The data supports the view that the Hong Kong Police force is committed to training highly capable officers and invests significant resources in professional training to build expertise in fighting Internet based crime.

---

[352] See Hong Kong Police. [Online] [Cited 15/05/2008]. Available from: < http://www.police.gov.hk/hkp-home/english/recruitment/salary.htm>.
[353] Jiao, A.Y. (2007) Ibid.
[354] Transcript 7 (HK): p.3.

(iv) Police Resources

The capacity to investigate and train officers in computer crime is directly related to resources. As a police officer from the TCD put it: "*If the police organisation was not supportive with resources, we cannot increase from 90 odd police officers to over 200 odd police officers, and everyone has their own computer*".[355] In an interview for this thesis, a specialist computer crime prosecutor from the Department of Justice also pointed out that his department received requisite resources to investigate computer related crime:-

> "*More and more, police are trained. In the past few years, the numbers have increased substantially. Lots of funds have been put there. Lots of police officers attend training courses, and I think it's a good sign.*"[356]

A chief inspector from the TCD interviewed for this thesis explained that the budget allocation for the TCD was very high. This budget allocation also allows the TCD to develop innovative investigation and policing techniques. A Chief Inspector from the TCD said:

> "*We maintain a very large budget for the procurement of the IT tools, for hardware and software. We also develop our own tools, you know, forensic tools, apart from others, open source tools, such as hardware and software that you could buy on the market. We discover that because a lot of things with tools are developed by the Western countries, some of them cannot address some of the problems, i.e. Chinese Characters, so we, in collaboration with the University of Hong Kong, develop our own forensic tools. It is called the Indigenous Abacus Search Tool and have given it to other law enforcement agencies for trial. It is very much the Encase tool, but addresses issues with Chinese characters. So, that is being continuously developed. This is one way the HK Police enhance the use of IT to solve crime.*"[357]

[355] Transcript 5 (HK) (In Chinese): p. 8.
[356] Transcript 2 (HK): p.4.
[357] Transcript 8 (HK): p.9. In 2005, the police announced that this was the world's first self-developed multi-language Digital Evidence Search Kit (DESK).

Another Chief Inspector from the TCD interviewed for this research explained that the TCD budget was approved at very high levels:

> "*Every 3 months there is a meeting in the Technology Crime Steering Committee that is attended by the head of the TCD and a few other senior officers in the TCD. In fact, it is very unusual for the senior commissioner [Director of Crime and Security] to chair the meeting that is connected with the work of a division. We are 1 of the 5 divisions. Having a very senior officer to oversee our work is very unusual. That also reflects how important senior management look at our work. This steering committee sets the directive for the TCD, i.e. for education, training, investigation, detection and PR. However, how to implement those strategies is up to us, and also the whole of the TCD comes up with the budget. We put up the estimate, after the scrutiny both by the bureau and the senior management, then the [money] provisions will be made on what we have asked for. The only body overseeing our work is the steering group, so we enjoy a degree of autonomy in that respect.*"[358]

This suggests that police senior management are serious about increasing the capability of the TCD. As aforementioned, in the 1990s, the police commissioner instructed the police to boost their investigative capability in computer crime by increasing manpower and financial resources. Because the Hong Kong police force is a traditional, top-down organisation, any order from the commissioner will be followed throughout the force. As a Sergeant from the TCD interviewed for this research said, "*I have been a police officer for over ten years now. The instruction inside the Hong Kong Police is one way from the top. Once the top man gives the order, everybody within the police has to carry out the order*."[359]

[358] Transcript 8 (HK): p.8.
[359] Transcript 6 (HK) (In Chinese): p.6.

The Hong Kong government is closely associated with business and government policy puts business interests first. As a result, economic crime is a government and policing priority. Because the police are an arm of government, the government can directly instruct the police as to their priorities. Because Hong Kong is not a democratic society, neither the government nor the police need account for, or justify, their priorities to the public. The police commissioner is directly appointed by, and reports to, the Chief Executive of Hong Kong. The commissioner can also go directly to the Chief Executive to seek an informal agreement on funding before submitting a formal funding proposal to the Legislative Council Financial Committee. After the government decided that police priorities should include Internet related economic crime in the 1990s, funding for the TCD has never been an issue. There is strong organisational and governmental support for the TCD in terms of manpower and equipment. As a chief inspector from the TCD stated in an interview for this thesis, "*We do not see much resistance at the [top] management level. They are very supportive*".[360]

The continuous flow of financial support is one of the keys to the TCD's success in maintaining its computer crime capability. For example, in 2001, the TCD invested more than HK$10 million in building a world-class computer forensic laboratory to upgrade its computer forensic services.[361] In 2005, the police further enhanced their capabilities in computer forensics. In the same year, the TCD organised a two-week, internationally recognised, computer forensics certification course, attended by 18 selected officers. The course was held at the

[360] Transcript 8 (HK): p. 9.
[361] Ng, M. (2001, 08-8) Ibid.

new HK$1.7 million technology crime training suite at the police headquarters in Arsenal Street.[362]

Having the right resources (time, money, facilities and staff) also allows the police to deal with complex and lengthy investigations. The head of the TCD interviewed for this research noted that:

> "*Once we've got the computer forensic evidence to prosecute or prove against the crime, it's not that big a problem in Hong Kong, because we can take our time. The longest computer forensic examination took about nine months, involving a case of the computer networks, ISPs, 80 computers and two Internet servers. We just closed them down and seized it, brought them all back here [to the TCD computer forensic laboratory] and rebuilt the [entire] system in here at the lab. Then, we examined it for nine months.*"[363]

This investment has pay offs in terms of developing expertise and enabling complex digital evidence to be prepared for the prosecution. A Superintendent of TCD interviewed for this research observed that:

> "*If you look into the electronic evidence by itself, it is a weave or weaves, layers of information. So it depends on which layer you are looking, whether you look at the high level which basically you just want to recover a main, an e-mail, or you just want to look at a word document to find some information. Or whether you need to analyze a log, analyze the firewall log, the intrusion detection log. Etc…or another possibility is to see the log has been altered. So, it depends on what level you are aiming to collect those digital evidences.*"[364]

---

[362] ISD, (2005, 06-07) Hong Kong Government. In May, local banking regulators and the banking association launched an initiative against online bank fraud to boost online banking customers' confidence. The HSBC's initiative involved distributing a one-time password security device to its online customers in Hong Kong. The device generated a time-sensitive, single-use six-digit security code for use when logging on and for selected online transactions. A hacker who somehow managed to intercept information disclosed during an online transaction would be unable to re-use it. See Beckerling, L. (2005, 06-09) 'Cyber theft forces lenders to reboot e-banking', South China Morning Post, p. Biz 7.

[363] Transcript 7 (HK): p.5.

[364] Transcript 4 (HK): p.3.

As a result, the TCD has achieved a number of notable successes at trial. In October 2005, the South China Morning Post[365] reported the world's first criminal conviction for copyright theft using Bit-Torrent technology (peer to peer sharing).[366] In this case, Chan Nai-Ming (alias 'Big Crook') was convicted by the Tuen Mun Magistrates' court for attempting to distribute three Hollywood films using Bit-Torrent. The police charged Chan with theft offences that carried a custodial sentence of up to four years.[367] This was a coup for the police, as peer to peer file sharing is a very new, complex and sophisticated technology that can involve thousands of individual personal computers in different places. As Richard Turnbull, policy co-ordinator for computer crime in the Department of Justice, stated, "*The prosecution of infringers (peer to peer file sharing) takes a lot of time and money and necessitates the seizure of computers at the home of each infringer*".[368]

Accordingly, this case demonstrated that the Hong Kong police have the expertise and the finances to do successfully investigate these types of technologically based crime. (**Cases 5**, **7** and **11** in the case study also demonstrate that the police can successfully complete complex and lengthy

[365] Shamdasani, R. Biggs, S. (2005, 10-25) 'The world's first criminal conviction of a BitTorrent', Hong Kong: South China Morning Post.
[366] Bit-Torrent or peer to peer sharing technology is a very efficient way of sharing large data files, because this file sharing technology can split the 'Bit-Torrent' file into small packages which can be downloaded independently. For example, if a user has made a file available, a peer may make a request to download it from the user (this person is called a 'leech'), but the person (as seed) who is downloading the files is also sharing the file with others who request the file. This means that ten to twenty people may be sharing the same file at the same time, with each one having certain bits of the file. Bit-Torrent file sharing technology is no longer dependent on a single person's connection. Instead it uses a collection of connections.
[367] As Carnabuci, a partner at Freshfields Brukhaus Deringer said "[*the fact that] an individual could go to prison may provide a policy platform for the police to educate people that this kind of activity is theft*." See Shamdasani, R. and Biggs, S. (2005, 10-25) Ibid.
[368] The Department of Justice Yearly Review 2007, Hong Kong: DoJ, p. 60.

investigations). The TCD see themselves as amongst the best in the world. As a Chief Inspector from the TCD interviewed for this research said:-

> "*Having travelled and visited other law enforcement agencies around the world frequently, I will say HK Police is very good on e-policing. If we compare with the US, UK and Canada, HK is not far off the mark with e-policing.*"[369]

(v) Low Value and Trivial Internet Crimes

Given that investigating Internet based economic crimes can be expensive and resource-intensive, the question remains whether these highly-trained police agencies bother with low-level or low value crimes. In this case, it is reasonable to assume that the police will generally not pursue minor or low value Internet crimes. However, it is a policy of the Hong Kong police to prosecute *all* cases of Internet banking fraud, however minor, as a training exercise. In theory, therefore, all cases of Internet banking fraud will be investigated (for example, see **Cases 3** and **8** in the case sample). However, this does not mean that all cases of fraud are prosecuted. In practice, the police only pursue low value fraud when they want to make some sort of point or policy statement (see **Case 1)**.

Nonetheless, minor or low-value frauds are likely to be investigated to some degree simply because the banks have a duty to report all instances of fraud to the authorities. As a chief inspector from the TCD stated in an interview for this thesis, "*For economic fraud, we got co-operation from the bank*".[370] Therefore, these crimes are more likely to receive initial police attention. As a Police Superintendent of the Technology Crime Division interviewed for this research explained:

[369] Transcript 8 (HK): p.11.
[370] Transcript 8 (HK): p. 6.

> "*For all of the computer related frauds, I think the most important issue, firstly is … over the Internet, they are trying to rip off small amounts from each person, but by having the number of people huge, then you can get a pretty good sum of money from all these people. So, what happens is that each individual, they suffer only maybe couple of hundred dollars or less than a hundred dollar. But it does add up at the end of the day. This makes investigation quite difficult.*"[371]

In addition to investigating report crime, the police in Hong Kong pro-actively trawl the Internet to looking for instances of fraud and theft. The intelligence unit within the TCD comprises between seven and ten officers who work full-time scrutinising the Internet. The HKMA also proactively looks for instances of crime within the banking and financial industry (see **Case 5**).[372] As a senior specialist computer crime prosecutor of the Department of Justice interviewed for this research said:

> "*Recently there has been some sort of cases where there is genuinely a crime, but it's sort of trivial and you don't know how to put a price on that. Practically, I am talking about those online games. Now, online games, we all know that if you start playing that particular character acquired some sort of status in the game in terms of power, money, all of that. Now, some ah, you need that particular login name and password to access that character. There has been a gradual increase in reporting computer crime in that area, to say well my [game] character has been stolen. The point is first how do we quantify the loss? You can say it's loss of enjoyment. Alternatively, you can also say well I spent 80 hours, O.K. 80 hours in playing that character and it acquired to be as rich in the real world as Li Ka Shing. So it must be worth very much. The point is, if these sorts of crimes are continuing to increase, we all know it's a crime, but it's not the sort of crime which ordinary*

[371] Transcript 4 (HK): p.5.

[372] On 16 August 2003, the South China Morning Post newspaper reported that six hackers had been arrested for hacking into online games accounts. They had used the victims' passwords illegally to steal the points in an online game. However, in the same report, Senior Inspector Leung Ka-Wai, from the TCD stated that, "*The comparatively small arrest figure this year was related to the fact that many cases involved a 'crime scene'- the locations of the [Internet] servers of the online games outside of Hong Kong's jurisdiction, such as Taiwan and the United States*".

> *people will say it's a normal type of crime. You can't say to a victim it's trivial we are not going to investigate [it], right.*"[373]

In one example, on 10 November 2003, the Hong Kong government[374] reported that a 36 year old man had been charged with two counts of accessing a computer with dishonest intent, one count each of obtaining property by deception using a false instrument and possession of a forged Hong Kong Identity Card, in connection with online fraud involving two auction websites between January 2002 and November 2003. The police began their investigation after 29 online auction sellers had reported to the police that they had received dishonoured cheques, with a total value of HK$216,200 (approx. GBP15,897), from an online customer.[375] Using a false email address, the offender hacked into the Internet register and registered online as an auction buyer. After an extensive police investigation, the offender was arrested by members of the TCD on 8 November 2003. Although relatively little value was involved, the police still pursued this case of Internet fraud.

Another case shows that the police are willing to pursue minor cases for their deterrent value. This case concerned a man who posted a link to an overseas web-site showing adult pornography on online forums. He was charged under the Control of Obscene and Indecent Articles Ordinance for publishing obscene and indecent photographs. This was the first case that the TCD had prosecuted under

[373] Transcript 2 (HK): p.10-11.
[374] Information Service Department, (10/11/2003) 'E-auction fraudster charged'. Hong Kong Government, Press Release.
[375] GBP15,897 divided by 29, means that each victim lost GBP548 on average.

the Control of Obscene and Indecent Articles Ordinance.[376] The Kwun Tong Magistrates' Court convicted Woo Tai-Wai for publishing eight obscene photos via a local Internet forum. This case caused quite a shock amongst the netizens in Hong Kong, with many commentators questioning the motives of the police. They said that:

> *"Yahoo and Google carried links to porn sites. In cases where search engines list out all the links to pornographic websites, is it justifiable to ask whether these would have to undergo censorship as they also provide these hyperlinks to obscene articles? We are not encouraging the distribution of this kind of material, but I suggest more guidelines from the government for internet users."* [377]

Some people saw the case as an example of a 'moral crime' and not something that should be prosecuted by the police. The police, however, clearly regarded the matter as sufficiently serious to investigate and prosecute for policy reasons.

Summary

Since the 1990s, the police have made major headways in tackling Internet crime and invested significant amounts in resources and training. The Hong Kong force now compares itself to the best in the world in this field. Moreover, despite the expense involved, the police apply these specialist skills and resources to low-value economic Internet related crimes. Unlike most common law countries, where the police and prosecution have introduced informal thresholds for investigating fraud, (the value of the fraud must pass this threshold, before the

[376] Wong, C. and Tsui, Y. (11 May, 2007) 'HK$5,000 fine for net porn link'. Hong Kong: South China Morning Post.
[377] Ibid.

crime will receive attention) these cases suggest that the Hong Kong Police do not have such a threshold.

Nevertheless, the prosecution may do. As a specialist computer crime prosecutor from the Department of Justice interviewed for this research said

> "*It comes to resources; it's a matter of allocation by prioritisation. If we have too much work to do, we would it's too trivial we would put it back a little bit… if it's a trend, that trend will go away shortly, right!*"[378]

The DoJ is differently resourced than the police. As the public prosecutor, the Department of Justice is responsible for the conduct of criminal proceedings.[379] Pursuing 'trivial' cases may be costly and attract public and/or judicial criticism if the cases go to trial. The Department of Justice also has its own prosecution thresholds, one of which is whether the prosecution is in the public interest. An expensive prosecution of a trivial case may not be considered in the public interest. The Department of Justice might decide to pass the case file back to the police with a recommendation to amend the charge, impose an alternative charge or simply discontinue the case. As a specialist computer crime prosecutor from the Department of Justice stated in an interview for this research said,

> "*We may need to go the police station to ask them to [bring charges or clarify the evidence] to us, so that we can understand…Because we are part of the prosecution team*".[380]

[378] Transcript 2 (HK): p.11.
[379] The independence of the Department of Justice is constitutionally guaranteed by Article 63 of the Basic Law of Hong Kong, which stipulates that the department, "shall control criminal prosecutions, free from any interference". See The Basic Law of HKSAR. Article 63, also see DoJ, The Statement of Prosecution Policy and Practice. [Online] [Cited 14/03/2007]. Available from: <http://www.doj.gov.hk/eng/public/pub20021031con.htm#6>, para. 1.1.
[380] Transcript 2 (HK): pp. 1 and 6.

If the Department of Justice do decide to accept an Internet banking fraud case for prosecution, the case file must first go to a specialist unit called the commercial crime and corruption unit (CCCU).[381] This specialist unit, which consists of 26 specialist prosecutors, including computer crime specialists, acts as an initial filter within the department. Members of the unit prepare and prosecute cases submitted by the CCB, the ICAC and the Customs and Excise Department. However, the decision whether or not a case is prosecuted remains within the Department of Justice. In sum, although major resources are put into the recruitment and training of specialist police, and cases of Internet banking fraud are thereby more likely to reach the prosecution stage, the policies, resources and decision-making at the prosecution stage ultimately decide if a case is actually prosecuted at all.

[381] Department of Justice. Op Cit.: p. 83. The CCCU's key duties include preparing legal documents, preparing statistics and handling pre-trial issues, such as providing evidence to the specialist prosecutor to make a decision on whether there is a real chance of conviction against the defendant. If not, the specialist prosecutor can make a discretionary decision not to continue with the prosecution, to request further information from the police or to amend the charge. Whether the case proceeds to a full contested trial depends on the seriousness of the case and the nature of the charges. The majority of criminal cases are heard in the Magistrates' Court. Some are heard in the District Court or the High Court, depending on the value or the seriousness of the case. There are three possible outcomes for the prosecution in court. The defendant may be convicted or enter a guilty plea and sentence may be imposed by the judge. If found not guilty, either because the case fails on technical grounds or on the merits of the evidence, then the case will be recorded as crime, but not as a conviction. Moreover, since the handover in 1997, the number of criminal court proceedings in Hong Kong that have been heard in Chinese (mostly in Cantonese) has increased dramatically.

# Chapter Nine
# Sample of Hong Kong Cases

Introduction

In the preceding chapters, I have examined in detail the key factors that have shaped the priorities of (i) the Hong Kong government; (ii) the police; and (iii) the banks in regard to economic crime, including Internet banking fraud. I have also looked at some of the reasons why not all cases of Internet fraud make it to trial stage. As a specialist technology crime prosecutor from the Department of Justice interviewed for this research explained:-

> "*Hong Kong is different from many countries in the West. For example, the USA is a large country, therefore, it is very popular for people in the States to buy things over the Internet whereas Hong Kong is geographically a small place - just spend two minutes or five minutes and you are in a shop. That's the reason why I think we don't really have many cases. ... in the States in a lot of cases, they do it fun. For example, hacking into the FBI [website], well just to deface it for one minute. If that particular guy managed to deface the FBI website, then he can show off to his friends. That, that's different. I haven't seen that in Hong Kong. For e-fraud, as I said, they attempt to sell one item to a hundred people, get the money and then they're gone. That's sort of more extensive overseas and [in Hong Kong] they are really [after] serious money when they commit that offence. I think that's the main difference.*"[382]

Several police officers interviewed for this thesis stated that there were relatively few cases of Internet banking fraud in Hong Kong. However, as I have shown, the cases that do make it to the trial stage are likely to be the tip of the iceberg. According to a chief inspector of the TCD interviewed for this research, "*a lot of Internet related crimes happen, such as online shopping fraud or auction fraud*

[382] See Transcript 2: p.5.

*and e-banking theft…*"[383] Sometimes the victims in such cases do not want to report the crimes to the authorities. As a result, these cases remain part of the 'dark figures' on under reported Internet related crime. Sometimes such cases are dealt with by private investigators who report to the police only as last resort. According to a Regional Director for security of a global credit card company:

> "*…most of the private sector investigators, if they come across any computer crime cases, they really want to refer the case to the police but that will take some time, so they prefer to cover or conclude the cases by themselves at the very beginning until if they think that oh the law is so huge they need to ask the law enforcement people to prosecute some person then they will refer to. Otherwise, I would say most of the cases are not reported.*"[384]

Although a great deal of money, time, and skill is spent on investigating Internet based economic crimes, not all cases result in a trial, even though most cases are likely to be thoroughly investigated. Even fewer cases reach the Appeal Court. Nonetheless, appeal court cases provide one of the few sources of information on what the courts are doing. In this chapter, I analyse the Internet banking fraud cases that have gone to trial and then been appealed within a specific period. In all, these cases reveal that the policing of economic Internet crimes in is influenced by Hong Kong's (i) political structure as a non-democratic, semi-authoritarian city state; (ii) free market economy; (iii) legal environment; and (iv) local technological and financial savviness and (v) the increase in mainlandisation after 1997. Furthermore, the case samples provide evidence of:

(i) the liaison between the banks and the police;

[383] Transcript 8 (HK): p. 1.
[384] Transcript 10 (HK): p.10.

(ii) the capability of the police in investigating complex cases of Internet banking fraud, especially international cases;
(iii) the police use of the Computer Crimes Ordinance 1993;
(iv) whether the rule of the law is applied equally or just a few high profile cases are sent to trial;
(v) the mainlandisation of Internet banking crime; and
(vi) how the courts sentence these kinds of cases.

In analysing the case sample, I follow the methodology established by T. Wing Lo and Paul Ngan in their 2009 article, published in *Crime, Law and Social Change*.[385]

Computer Crime Ordinance 1993 (C C Ord. 1993): An Analysis of Cases

My sample of cases were tried and went to appeal between 1999 and 2012, well after the Computer Crime Ordinance came into force in 1993. All of the cases were identified using the Westlaw Hong Kong reported case database. The sample consists of the fifteen cases that went to appeal between January 1999 and June 2012. All were dealt with originally by the Magistrates' Court. The main features of the 15 cases are listed in Table 9.1 below.

*Case 1: HKSAR v Tsun Shui Lun-[1999] 2 HKC 547, Magistracy Appeal No 723 of 1998*
*Case 2: HKSAR v Tam Hei Lun & ORS-[2000] 3 HKC 745, Magistracy Appeal No 385 of 2000*
*Case 3: HKSAR v Choy Yau Pun-[2002] 4 HKC 309, Magistracy Appeal No 450 of 2002*
*Case 4: HKSAR v Lai Mei Yuk [2004], Criminal Appeal No 427 of 2003*
*Case 5: RE Chen Kam Chiu and Others-[2005] HKCU 987, CACC 179/2004 (On Appeal HCCC No 158 of 2003)*

[385] See T. Wing Lo, Paul Ngan, (2009) 'Restricting loans of money to Hong Kong civil servants: social censure or violation of human rights?' *Crime, Law, and Social Change*, Springer 52, pp. 385-403.

*Case 6: Chiu Hoi Po v Commissioner of Police-[2006] HKCU 681, HCAL 105/2003*
*Case 7: HKSAR v Leong Wai Keong-[2008] HKCU 1915, Court of Appeal CACC 476/2007*
*Case 8: HKSAR v Kam To Fung-[2008] HKEC 1041, Magistracy Appeal No 565 of 2007*
*Case 9: HKSAR v Marimuthu Jaisanka-[2008] HKCU 243, Court of Appeal CACC 403/2007*
*Case 10: HKSAR v Ho Ching Wah-[2009], Court of Appeal CACC 106/2008*
*Case 11: HKSAR v Ma Hon Kit Sammy & ORS-[2010] HKCU 2189, Court of Appeal CACC 148/2009*
*Case 12: HKSAR v Cai Zhaorong-[2012], Court of Appeal CACC 365/2011*
*Case 13: HKSAR v Chan Wai Ming-[2012] DCCC 137B/2011*
*Case 14: HKSAR v Cheung Yiu Ming-[2012] DCCC 320/2011*
*Case 15: HKSAR v Yaghi Jose-[2012] DCCC 141/2012*

All the cases were initially investigated for offences under the Computer Crime Ordinance 1993. In **Case 9**, the defendant pleaded guilty in the District Court for an offence contrary to section 25 of the Organised and Serious Crimes Ordinance, Cap. 455. In **Cases 5-15**, the defendants were initially investigated by the authorities for offences under the Computer Crime Ordinance 1993, such as unauthorized access to the Internet. However, at trial, the actual indictments were for other offences, some of which were far more serious. So, for example, in **Cases 7, 9, 13** and **15** the indictments at court, which included dealing in stolen property, differed from the initial police charges.

In **Cases 7**, **9** and **13**, the accused were found guilty. In **Case 15**, the court concluded "not without reluctance", that there was reasonable doubt and the accused was acquitted of dealing in property known or reasonably believed to represent the proceeds of an indictable offence because the prosecution failed to prove the case beyond reasonable doubt.

All case involved the use of the Internet and gaining unauthorised computer access, and all but one involved personal monetary gain (**Cases 2-15)**. In **Cases 2, 3, 4** and **9**, the defendants pleaded guilty at the trial, but later appealed their sentences. In **Cases 13** and **14**, the defendants were found guilty after a trial at the District Court. In **Case 15**, the defendant was found not guilty at trial. I discuss these and the rest of the cases in detail below.

## Table 9.1 Features of Computer Crime Ordinance 1993 Cases

| Feature / Case No. | Initial Offence investigated under C C Ord 1993 | Actual Indicted Offence in Court | Advantage | | Mainland China Connection Victim/ Defendant | Committed the crime via Internet | Victim Not blood/ Close related | Appeal | Other offences involved |
|---|---|---|---|---|---|---|---|---|---|
| | | | Monetary | Non Monetary | | | | | |
| 1 | yes | CC Ord 1993 | | yes | no | yes | yes | yes | |
| 2 | yes | C C Ord 1993 | yes | | no | yes | yes | yes | copyright |
| 3 | yes | C C Ord 1993 | yes | | no | yes | yes | yes | theft |
| 4 | yes | C C Ord 1993 | yes | | no | yes | yes | yes | |
| 5 | yes | Conspiracy to defraud | yes | | yes | yes | yes | yes | |
| 6 | Police Internal Tribunal | Conduct calculated to bring public service into disrepute | yes | | no | yes | yes | Judicial Review | |
| 7 | yes | Dealing in stolen property | yes | | no | yes | yes | yes | Money laundering |
| 8 | yes | Handling stolen goods | yes | | no | yes | yes | yes | |
| 9 | yes | Dealing in stolen property | yes | | no | yes | yes | yes | |
| 10 | yes | Theft | yes | | yes | yes | yes | yes | |
| 11 | yes | Insider dealing | yes | | yes | yes | yes | yes | |
| 12 | yes | Theft | yes | | yes | yes | yes | yes | |
| 13 | yes | Dealing in stolen property | yes | | yes | yes | | no | |
| 14 | yes | Fraud, theft and soliciting advantage | yes | | yes | yes | yes | no | corruption |
| 15 | yes | Dealing in stolen property | yes | | yes | yes | yes | no, not guilty at the trial | |

**Table 9.2 Number of Defendants in Each Cases**

| Case No. | Nos. Defendant | *M/F | Guilty | Not Guilty | Custodial Sentence |
|---|---|---|---|---|---|
| **1** | 1 | M | 1 | | no |
| **2** | 3 | M | 3 | | 3 |
| **3** | 1 | M | 1 | | 1 |
| **4** | 1 | M | 1 | | 1 |
| **5** | 5 | M | 5 | | 5 |
| **6** | 1 | M | Disciplinary tribunal found against the defendant | N/A | no |
| **7** | 1 | M | 1 | | 1 |
| **8** | 1 | M | 1 | | Initially no, then reduced to fine on appeal. |
| **9** | 1 | M | 1 | | 1 |
| **10** | 2 | F | 2 | | 2 |
| **11** | 5 | 2 were F | 5 | | 2 |
| **12** | 1 | M | 1 | | 1 |
| **13** | 1 | M | 1 | | 1 |
| **14** | 1 | M | 1 | | no, acquired on appeal |
| **15** | 1 | M | | 1 | no |
| **Total** | **26** | | **24 (92.3 per cent)** | One not guilty; one is not a crime , a judicial review case | **18 (75 per cent)** |

*Male=M, Female=F.

Common Features

The following nine features are common to the majority of the cases. These are listed above at Table 9.2:

(i) Almost all cases (**Cases 1-5** and **Cases 7-15**) were initially investigated by the police under the Computer Crimes Ordinance 1993 but then prosecuted as a different offence.
(ii) Apart from **Case 6**, all went to trial. In Case 6, the appellant appeared before a police internal disciplinary tribunal, before appealing via judicial review.
(iii) All defendants used the Internet to commit the offences.
(iv) None of the defendants were related to their victims.

(v) Almost all (13 out of 15) the cases were appealed, mainly against their sentence, except **Cases 13** and **14**.
(vi) Almost all of the accused (24 out of 26 defendants, 92.3 per cent) either pleaded guilty or were found guilty at trial. In **Case 15**, the accused was found not guilty at trial.
(vii) In almost all cases, the motive was monetary gain (except **Case 1** where the motive was political).
(viii) There was a high rate of custodial sentences, with 18 out of the 24 defendants found guilty receiving a custodial sentence (75 per cent). The exceptions were **Case 1** (community service), **Case 6** (judicial review upheld his dismissal), **Case 8** (fine of HK$5000); and **Case 14**, where the conviction was overturned on appeal;
(ix) The defendants were mainly male (only 3 out of the 26 were female).

Distinctive Features

Apart from these nine common features, the cases share six distinctive attributes:

(i) Complexity of the case

**Cases 5**, **11**, **12**, **13**, **14** and **15** were all complex cases. For example, **Case 11** included several complex crimes that involved the Hong Kong Monetary Authority (HKMA), and the Securities and Futures Commission (SFC). The accused were prosecuted by the SFC for insider dealing using an Internet bank account to deal in shares. The five defendants in the case were all closely related. The first defendant was employed as a senior executive (vice president) in an investment bank. He was handling a project relating to the privatisation of a company listed on the Hong Kong Stock Exchange and possessed important price-sensitive information. He deliberately leaked the sensitive information to his brother, the third defendant, who then passed it on to the other relatives. Based on the information gained from the third defendant, the second, fourth and fifth defendants bought large numbers of shares via their HSBC Internet bank accounts (over 1.6 million shares at between HK$1.58 and HK$1.60). They did this within a 15-minute period. Two weeks later, the privatisation of the listed company was announced, with a cash offer of HK$1.80 per share. The defendants

thus profited from their share holdings. The authorities were alerted to the case because the volume of shares that were traded within the fifteen minutes constituted 93 per cent of all the shares traded in the company on the stock exchange that day (6 June 2006).

This case highlights the fact that the Hong Kong authorities keep a watchful eye on the Hong Kong financial markets and the banking system for abnormalities such as this. It also highlights the fact that Internet bank accounts in Hong Kong are not only used for simple, personal money transactions, but can also be used for the online trading of stock and shares involving large sums of money.

By prosecuting this case, the authorities sent a clear message to others contemplating committing this type of crime. These actions enable the authorities to help protect the integrity of the Hong Kong Internet banking system and the stock market. As the judge stated in this case, "…*the electronic banking system and a 'clean' stock market is vital for Hong Kong*".[386] This landmark case was widely reported in the media as it was the first insider dealing case to involve a prison sentence since insider dealing was made a criminal offence under the Securities and Futures Ordinance in 2003.[387] Ma was given a sentence of 26 months and his girlfriend 12 months, while his nephew received 200 hours community service and a fine of HK$17,000.

I have argued that protecting Hong Kong's status as one of the world's leading capital markets is an important priority for the government and the police. As

[386] See HKSAR v Ma Hon Kit Sammy & ORS-[2010] HKCU 2189, Court of Appeal CACC 148/2009.
[387] Security and Futures Commission, Chief Executive Officer, Mr. Martin Wheatley.

Hong Kong is one of the world's leading capital markets, the stock exchange and the related financial industries provide a huge source of income for the government in term of tax. In recent years, the Hong Kong Stock Exchange has also begun to serve as a hub for mainland Chinese companies seeking to raise capital and a channel for listing on the open market. Today, more than 50 per cent of the stocks listed in Hong Kong are for mainland Chinese companies. In 2012 alone, 62 mainland companies were newly listed on the Hong Kong stock exchange, raising over HK$90 billion.[388] Therefore, this case seems to confirm that the courts take a harsh view of activities that have the potential to damage Hong Kong's economy and reputation. The case also provides evidence of the role of the HKMA in picking up suspicious transactions.

**Cases 5, 10, 12 and 13**, were also complex cases involving large amounts of money and a link to mainland China.

In **Case 5** *RE Chin Kam Chiu and 4 others*[389] all the defendants were found guilty in the Court of First Instance of a single count of conspiracy to defraud. At trial, the first defendant was sentenced to 6½ years, the second defendant to 4½ years, the third defendant 5½ years, and the fourth and fifth defendants to 4½ years. They all appealed their conviction and sentences.

Four of the appellants were officers of the Sin Hua Bank (a deputy general manager, a deputy manager in the credit department, an assistant general manager

[388] See Deloitte Touche Tohmatsu Report on Statistics on Mainland IPOs in 2012. Website < http://www.deloitte.com/view/en_CN/cn/Pressroom/pr/98b4f30f818fb310VgnVCM3000003456f70aRCRD.htm>. [Visited on 11/4/2013].
[389] See the judgment of High Court Appeal No. [2005] HKCU 987, CACC 179/2004 (On Appeal from HCCC No. 158 of 2003).

of the bills department and a senior manager in a sub-branch). In 2001, the bank merged with and formed part of the Bank of China, whose headquarters are in Hong Kong. The defendants used their positions as bank officers to apply for 25 letters of credit (L/Cs), amounting to HK$1.8 billion, using false documents, such as false cargo receipts and false bills of lading. One of appellants was the bank's in-house accountant. He signed the applications and used the Sin Hua Bank's Internet connected banking system to apply to the bank's Tsuen Wan bills centre, which issues credit documents, for the L/Cs.

This case was also connected to mainland China. As the prosecution stated, *"…these 25 letters of credit, although they were opened in Hong Kong through the Tsuen Wan Bills Centre, and although the Applicants' accounts were dealt with at the Castle Peak Road sub-branch of the Sin Hua Bank, these particular L/Cs were channelled through Shenzhen and drawn on the Shenzhen Branch credit lines of the Sin Hua Bank*". Although one defendant suggested that the Shenzhen branch was a separate legal entity, the court said there was no doubt that the defence were aware of the prosecution's allegations that the Shenzhen branch was an integral part of the Sin Hue Bank group. According to the court documents, the bank was a limited liability company registered in mainland China with its headquarters in Beijing. All the issued shares in the bank were owned by the Chinese government. The court added that the fact the Shenzhen branch was outside the HKMA's control was unrelated to the real issue in the case, as there was unity of management and control between the Hong Kong and Shenzhen branches.

The case came to light in April 1998, when the HKMA expressed concern over the bank's exposure to the Keen Lloyd Group (which was owned by the appellants and operated in mainland China). The exposure of HK$1.8 billion was approximately 25 per cent of the bank's capital. At the same time, the HKMA also expressed concern that the bank's credit line to the Keen Lloyd Group had increased 50 per cent since 1997. The HKMA requested that the bank reduce its exposure to the Group. Eventually, the case was referred to the police and the ICAC for investigation.

The defendants' appeals against their convictions and sentences were dismissed.

This case also illustrates something mentioned by Linklaters in their 2010 overview of the role of the FSC in investigating and prosecuting insider dealing. They said that over the past two years, they had:

> "*... seen a paradigm shift in the approach adopted by the Securities and Futures Commission (SFC) in its investigations, with use being made of previously untested statutory powers to freeze assets, compel production of documents and record interviews with employees. Insider dealing has been top of the SFC's agenda throughout. However, it was not until 2008 that the SFC brought its first criminal prosecution for insider dealing (some five years after the offence was added to the statute books). The convictions of five individuals in the case of HKSAR v Sammy Ma Hon Kit and others (Criminal Appeal no. 148 of 2009), one of whom was a banker who passed inside information to his girlfriend and family in relation to a deal on which he was advising, were secured over a year later. Fines were imposed on each and sentences of imprisonment were passed in respect of the two main parties. Last month, Hong Kong's Court of Appeal refused leave to appeal against the convictions of two of the five. The Court of Appeal was satisfied that the irresistible inference to be drawn from the trading activities of these family members*

> *was that they had received inside information from the banker.''*[390]

Linklaters also pointed out that many such cases had previously been dealt with via the civil – not criminal – legal process:

> "*… other insider dealing cases have been handled through the Market Misconduct Tribunal (MMT), a specialist civil forum with enhanced 'penalty' powers. Findings of insider dealing were made last year by the MMT against a banker and two fund managers who had traded ahead of a placement in which the banker was involved. The Tribunal recommended that the SFC impose disciplinary penalties on all three. The SFC subsequently revoked their licences for life. One of the fund managers did not appeal. The banker's appeal was determined last month by the High Court which reiterated the seriousness with which the courts view insider dealing as a form of dishonest misconduct, even where no immediate pecuniary benefit is obtained. The licence revocation was confirmed but reduced from life to a period of 10 years.*"[391]

(ii) Trans-jurisdictional cases

**Cases 5**, **10**, **12**, **13**, **14** and **15** all involved a link between Hong Kong and mainland China, while **Case 12** involved Hong Kong, mainland China and a minor connection with the US. **Case 14** stretched between the US, mainland China, Hong Kong and Europe; while **Case 15** involved Hong Kong and Dubai. Nonetheless, as the head of the TCD confirmed in an interview for this thesis, even though these cases were trans-jurisdictional, the perpetrators were still within the reach of Hong Kong law:-

[390] See Linklaters, Regulatory Investigations Update,(Nov. 20th 2010). Website: <[http://www.linklaters.com/pdfs/mkt/lit/Regulatory_Investigations_Update_November2010.pdf, online visited 27/5/2013], Visited 27/5/2013

[391] Ibid.

> "*In Hong Kong we are trying to do something on the crime jurisdiction ordinance (CJO), so that if a criminal in HK is doing something wrong overseas HK law and jurisdiction can try the crime. On the other hand, if somebody is doing something wrong in HK from overseas the law can also try this person too. However, we still have quite a long way to go, if you look at the European Cybercrime Convention, the Interpol best practice, there were a lot of big principles, but because those principles are too big, nobody really follows it.*"[392]

He went on to say:

> "*The way we look at the moment, a lot of those Internet commercial crimes that occur here are not posted in HK; it was somewhere else. If you look at HK geographically, because it is so small, if anything comes up, we can close it up within one day. Last Friday, there was a report of an advance fees scam in Kowloon, on Saturday morning I sent my men down there to seize the server and closed it down. We can do that. However, a lot of the international fraudster, they are not locating their servers in Hong Kong, they locate their servers somewhere they think is safe and the police there in not up to it. So, they host their web around the world. So, a lot of these activities are international, but it can also affect HK…you might not know that one case loss HK$1.3m on e-banking, however, we stop it in time, so the loss zero…*"[393]

Another respondent, a superintendent in the TCD, also explained how the TCD had established international networks, which they could call on to assist them in investigating trans-jurisdictional crimes should they need it. He said:-

> "*I think basically we participate in a lot of international seminars, talks, there are a lot of inter-field working groups where different police organisations get together, share information, know each other, establish our intelligence, establish our contacts. So that, if there is any special case, we can liaise directly to obtain the information. If International Mutual Assistant is*

[392] Transcript 7 (HK): Pp.7-8.
[393] Transcript 7 (HK): p.13.

> *required, then we'll proceed through IMA in mutual goal assistance.*"[394]

The head of the TCD explained some of steps that might be needed before solving such a case:

> "*There are a lot of important issues, when you are looking at this kind of thing. First of all, in our speed: how fast we can obtain the electronic data, such as the computer record, IP record? It is very difficult for us to obtain record when it is trans-border. Often it is the time - we get all information but it is too late. Put it this way, we settle down several issues, first of all, technical issues in getting the evidence, secondly, after getting the record from whoever that is (the person) and assistance from whoever that is. Can we get the computer forensic evidence to prosecute or prove against the crime – that is not that a big problem in Hong Kong, because we can take our time. The longest computer forensic examination took about nine months, involving a case of the computer network, ISP, 80 computers and two internet servers. We just closed them down and seized it, bought them all back here and rebuilt the system in here at the lab. Then, we were examining it for nine months. After the first three months, we said we can't handle it; we asked Microsoft to assist us. So after nine months, we got everything we wanted, so we prosecuted the persons involved… if the case occurred locally, then we can easily do it, but if it is something on overseas, then we will have problem*." [395]

(iii)The Mainland China – Hong Kong connection

Seven out of the 15 cases in the sample had a Hong Kong/mainland China link, namely, **Cases 5**, **10**, **11**, **12**, **13**, **14** and **15**. This trend was confirmed by an Internet banker in an interviewed for this thesis who said:-

> "*… Hong Kong is growing into… a city of China. We are still running a different system, unlike the mainland China, but economic activities are more likely to be related to the mainland Chinese. Now this kind of activity is happening within the region, what we call the greater*

[394] Transcript 4 (HK): p.4.
[395] Transcript 7 (HK): p.5.

> *China region, so the situation is getting more complicated… Internet or the electronic crime will grow and tackling it will be more difficult. Talking about, like, across region or going to mainland China, their system or systems for tackling this kind of thing are more problematic as well.*"[396]

**Case 10** (HKSAR v Ho Ching Wah-[2009]) involved two defendants who were accused of the theft of HK$9.35 million and furnishing false information using an Internet account. One of the defendants worked for a company (Silverart HK) that did business with a company called SilverArt (Quan Zhou) in mainland China. The defendant withdrew money from the Hong Kong company's bank account for her own use and covered this up. The company's owner travelled regularly to China. When the owner was out of Hong Kong, he would tell the defendant the password to the company's Internet bank account over the phone and they would then complete transactions on the Internet. In 2004, the defendant became sick. Around this time, the owner became suspicious of the shortfall in company funds and discovered that the missing money had been paid into the bank account of the defendant and a second defendant, who was involved with Silverart Shenzhen. In the course of the offence, Hong Kong bank-notes were exchange for renminbi in face to face cash transactions. In 2005, the owner reported to the police that the company had suffered losses of HK$9.35 million.

In **Case 12** (Cai Zhaorong-[2012]), which involved US$823,896 (approximately HK$6.43 million), the defendant was indicted for theft rather than Internet banking fraud. The case was prosecuted in Hong Kong, although the defendant lived and worked in mainland China. The defendant held an Internet bank

[396] Transcript 9 (HK): p.8.

account at an HSBC branch in Hong Kong in the name of U-way Electronics Company Ltd. and was the sole director of this company. On 18 June 2010, a bank in the US mistakenly transferred US$823,896 into the defendant's HSBC Internet bank account. At the time of the transfer, U-way had just US$11.72 in credit. The day after the erroneous transfer, the defendant used his HSBC account to transfer the maximum amount allowed (US$64,500, HK$500,000) to a bank account in Shenzhen city (just over the border in southern China). He also resigned his directorship of U-way Electronics and transferred all of his shares to a third person, who acted as a front man in negotiating with the US bank.

The defendant was arrested when he attempted return to Hong Kong. After a long negotiation, he fully repaid the stolen funds to the US bank, together with an amount to cover legal costs. At trial, the defendant pleaded not guilty but was convicted and given a 22 month prison sentence. He sought leave for appeal for his conviction and sentence, but was refused. The judge argued that it was a very serious matter and that the defendant had only repaid the victim at the last minute after a lengthy, expensive and uncertain period of negotiation. It was only at that point that the financial impact of the crimes had been to all intents and purposes nullified.

**Case 13** (Chan Wai Ming-[2012]) involved the transfer of HK$8 million from a Hong Kong dollar account into the account of a company in Shenzhen. The company existed only on paper. The defendant faced charges of money laundering under the Organised and Serious Crime Ordinance. The money was held in a Bank of China account and the prosecution alleged that large sums were

moved in and out of these accounts using Internet banking. The prosecution also alleged that the money represented the proceeds of crime, as it was gained from a conspiracy to defraud the Chinese authorities by obtaining cross-border vehicle permits with the help of a mainlander, Chan. The money was being transferred to Chan's company account in Shenzhen. The court regarded the scheme as fraudulent, as vehicle permits are only given to overseas investors who have set up a mainland company. The court found that the company was not a legitimate overseas investor. The judge specifically noted that a corrupt government official in mainland China (Jiangmen) had used bank accounts in Hong Kong to launder and obscure the illegally-gained assets.

**Case 14** also involved a complex set of internet transactions between mainland China and Hong Kong. The defendant was charged with fraud under the Theft Ordinance and with soliciting an advantage under the Prevention of Bribery Ordinance. He was employed as the technical director of a company that provided a platform for online payments and technical support for merchants in receiving payments from customers on the Internet. The company also cleared online credit card transactions relating to banks and financial institutions. These kinds of activities are encouraged by government initiatives on closer economic integration with mainland China.

The defendant was employed to set up a technical centre in Zhuhai City, in Southern China, to handle programme development on the mainland, as it was said to be cheaper to set up an office in China. The office was set up in 2007, with three or four staff, in the name of Richard Chan, a Chinese citizen. The

defendant admitted inflating the expenses of the Zhuhai centre and pocketing the difference (563,318.23 renminbi) by depositing it into his bank account.

In this case, the defendant was alleged to have solicited an advantage and corruption involving commission fees from a trade partner in the US through email. The US company was an automatic clearing house that shared 25 per cent of the profit generated by facilitating Internet payments. However, the defendant sent emails to the US company soliciting commission of 40 to 50 per cent.

The District Court judge dismissed the corruption charge, but convicted the defendant for fraudulently inflating an expenses claim. The case was investigated and brought to court by the ICAC. However, questions were raised about the admissibility of the evidence, as the ICAC officers were said to have conducted off the record interviews with the defendant. This became an important issue at appeal.

This highly complex case stretched between the US, Europe, Hong Kong and Zhuhai City in China. Electronic crimes are often intertwined with other types of crime and are often involve trans-border transactions that cross several jurisdictions. As such, they pose problems for the prosecuting authorities both in terms of their complexity and the cost of the cross-jurisdictional investigation (as discussed in previous Chapters). Moreover, it is often difficult to get a conviction in highly complex trans-border corruption cases that involve several countries, which often involve Internet technology. One difficulty for the prosecution is to prove the chain of evidence, as the evidence is likely to be enmeshed in traditional paper and electronic formats, which may be embedded in different

electronic files on the Internet or in folders lodged in different jurisdictions. Moreover, the defendants can intentionally destroy electronic evidence by erasing files.

**Case 15** involved an Indian businessmen trading in Zhejiang, China. The defendant brought US$30,000 of textile products from Zhejiang Dongsheng Dyeing and Printing Company, which he paid for through Internet banking. He received an email, purportedly from his employee, telling him to transfer the money instead to a particular HSBC account. He was later told that Dongsheng had not received the money. There were at least two similar instances involving companies in North Carolina and Dubai, and an accountant in Hong Kong. The prosecution alleged that the defendant fell out with his accomplices and came to Hong Kong to withdraw the money in person. However, on appeal, the judge pointed out that the money had all along been handled by Internet banking, so that there was no reason for the defendant to come to Hong Kong in person.

The case also involved an assistant manager in the financial crime section of HSBC, who gave evidence on security measures to prevent unauthorized interference with a computer account record. The fact this bank officer served as a court witness demonstrates that the police liaise closely with the banks in prosecuting such cases.

(iv) Prosecuted under Computer Crimes Ordinance 1993 together with other crimes

**Cases 2**, **3**, **7** and **14** were prosecuted under the Computer Crimes Ordinance 1993 together with other serious crimes, such as corruption, theft, money laundering and copyright. In all four cases the defendants were found guilty.

These indicate how difficult it is to isolate Internet banking fraud as a separate offence, which may be one reason why the numbers for this specific offence seem so low. That is, the rates for Internet banking crime are 'hidden' within other offences.

(v) Prosecuted originally under the Computer Crimes Ordinance 1993, but ended up at trial charged with other offences

In ten out of the 15 cases (**Cases 5 - 15**) (66.6 per cent) the accused were initially charged under the Computer Crimes Ordinance 1993 but ended up being prosecuted for other offences. **Case 6** however, was not a criminal prosecution, but a disciplinary hearing.

In **Case 5,** the accused was prosecuted for conspiracy to defraud; in **Case 7** the accused was tried for money laundering; in **Cases 8**, **9**, **13** and **15**, the accused were tried for handling stolen goods; in **Cases 10** and **12**, the accused was tried for theft; in **Case 11** the accused was tried for insider dealing; in **Case 14** the accused was tried fraud, theft, soliciting an advantage and corruption. These examples demonstrate that many of those who are initially charged with computer crimes end up being tried for traditional crimes such as theft and handling stolen property. In these cases, although the defendants used the Internet to commit the crimes, they were not prosecuted specifically for Internet crimes.

(vi) Motive not always monetary gain

In **Case 1**, the motive was political not monetary. In **Case 8**, which involved stealing game points, it was not that clear whether the accused simply wanted to play the casino game, or wanted to use the bonus points to win cash.

Other Observations

(i) The Use of Custodial Sentences

The Hong Kong courts appear to take a strong line on all kinds of Internet and computer-related crime, not just those involving large amounts of money. In Case 2, for example, the third defendant (a teenager) was indicted for computer crimes (copyright offences) which involved obtaining access to a computer with dishonest intent, under the Computer Crime Ordinance 1993 and dishonest gain contrary to section 161 (1) (c) of the Crimes Ordinance. According to section 161 (1):

> *(1) Any person who obtains access to a computer-*
> *(a) with intent to commit an offence;*
> *(b) with a dishonest intent to deceive;*
> *(c) with a view to dishonest gain for himself or another; or*
> *(d) with a dishonest intent to cause loss to another,*
> *whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.*
> *(2) For the purposes of subsection (1)"gain" (獲益) and "loss" (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-*
> *(a) "gain" (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and*
> *(b) "loss" (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has.*

Two of the defendants who pleaded guilty in the Magistrates' Court later appealed their custodial sentences. Both of the defendants were teenagers who had strong family support and their probation officers considered them suitable

for a community service order. One had been studying at the Open University and it was argued that a custodial sentence would disrupt his studying. However, dismissing the appeal, the appeal judge commented that a custodial sentence was neither wrong nor excessive, because "*Whilst it is true that the number of prosecutions in respect of s 161 offences is at present small, the damage which such offences can cause should not be underestimated.*"

He added that "*there have been less than ten prosecutions in relation to offences under s 161 and in those circumstances it is most unlikely that the full range of crimes which would fall within s 161 would now be known or appreciated*." The copying of copyrighted works and selling them to members of the public on the internet commercially - even part-time as a 'cottage industry', was a very serious offence.

The case where the defendants are sentenced to imprisonment are indicative of the tough stance on crime control in Hong Kong and the belief that imprisonment is justified both as a punishment and a deterrent in cases of Internet-related 'white collar' crime. In **Case 3**, for example, the defendant also received a custodial sentence after pleading guilty. He was charged with using a computer with dishonest intent to cause loss to another, contrary to section 161(1) (d) of the Crimes Ordinance. The defendant was convicted of theft in the Magistrates' Court for gaining unauthorized access to his employer's computer and defrauding the Internet service provider of HK$286.81. His appeal against his custodial sentence was dismissed despite a strong recommendation for community service. The appeal judge commented that although the offence only involved a small amount of money (HK$286.81), the defendant had betrayed the trust of the

customer who had delivered the computer to him for servicing. The judge ruled that a custodial sentence would deter such conduct and that a period of disciplinary training 'in a detention centre' would be beneficial to the appellant.

In **Case 4**, the defendant was convicted of using a false instrument (under s 73 of the Crimes Ordinance), fraud (s 16A of the Theft Ordinance), theft (s 9 of the Theft Ordinance) and accessing a computer with dishonest intent (s 161 (1) (c) of the Crimes Ordinance). She was sentenced to 2½ years in prison. However, because she made full restitution to the two banks that had lost money, her sentence was reduced by six months on appeal.

Similarly, in **Case 7**, the defendant received a three year and 11 month custodial sentence, after pleading guilty in the District Court to offences including money laundering through an Internet bank account from Hong Kong to Taiwan and South Korea. His appeal against his sentence was dismissed. The background to the case was that in 2001, the defendant lost HK$50,000 at a Macau casino. He borrowed HK$60,000 from loan sharks. In return, he promised to open a bank account for the loan sharks to use, which he did this when he returned to Hong Kong. In 2002, he then went to South Korea to open another bank account under instruction from the same loan sharks. In 2003, he did the same in Taiwan. He suspected that the accounts were connected with illegal businesses but said he dared not refuse the loan sharks' demands for fear that would trouble his family members. Within a period of less than two years almost HK$30 million had been laundered through the accounts. On appeal the court said, "*the judge was right to emphasise the international element involved as what the applicant did seriously undermined Hong Kong's status as a financial and banking centre. I wish to echo*

*what Mayo VP said in HKSAR v. Mak Shing…'there was an international element to the offences and…Hong Kong has to take a very serious view of such matters as its international reputation in not be sullied."*"[397]

Again, this case demonstrates that the courts take a harsh approach to any illegal activity that threatens to damage Hong Kong's financial standing.

The defendant in **Case 8** was born in mainland China, but had come to Hong Kong at an early age. He had been arrested at Hong Kong airport when he returned from Australia after graduating from university. He was charged with handling stolen goods under the Theft Ordinance. The defendant was said to have dishonestly received 379 credit card receipts from Watsons the Chemist, which had been given to him by a friend. In an interview, the friend was described as a 'crafty guy'. However, the defendant stated that he did not understand the Cantonese phrase as meaning "people who have some sly or cunning underlying motive". The court did not accept this. However, on appeal, it was accepted that there was no evidence as to what the expression meant.

The defendant had used the credit card receipts to open an online casino account to earn bonus points. Even though this amounted to a de facto act of defrauding the card-issuing bank via the Internet, the defendant was not indicted for Internet banking fraud but for theft. He was found guilty at the Magistrates' Court of handling stolen goods contrary to the Theft Ordinance, Cap 210, and was fined HK$5,000. On appeal, the judge was persuaded that the credit card receipts might

[397] See HKSAR v Leong Wai Keong-[2008] HKCU 1915, Court of Appeal CACC 476/2007.

not have been stolen, and the appeal against the conviction was allowed. This was unusual as in all the other Appeal Court cases the convictions were upheld.

In **Case 9**, the accused was tried for dishonestly accessing other people's Internet bank accounts under section 25 of the Organised and Serious Crime Ordinance. In this case, the third parties lost HK$3,198,000. Because the defendant pleaded guilty, his sentence was reduced by a third and he received 26 months.

In **Case 10**, the two accused were charged under the Theft Ordinance with theft and false accounting via the Internet. The first defendant was sentenced to 5 years and 3 months in prison and the second defendant to 12 months.

In **Case 11**, two of the five defendants received custodial sentences of 26 months and 12 months, respectively. These were the first custodial sentence for insider dealing in Hong Kong.

In **Case 12**, the defendant was convicted of theft totalling HK$6.4 million. He was sentenced to 22 months imprisonment. At appeal, the judge stated that, *"In cases of this kind there are no guidelines as to sentencing"*. However, because the defendant made full restitution, the sentence was reduced by 8 months.

This high number of convictions confirms the view of a front line police officer interviewed for this research, who said that:

> "a *high number of [computer related crimes] cases which go to court end with conviction verdict. Even though they*

*may appeal their verdict to a higher court, the higher court usually keeps the original guilty verdict"*[398];

In contrast to the lower courts' strong custodial sentencing, in **Case 1** the court of appeal overturned a prison sentence. **Case 1** highlights a particular characteristic of Hong Kong's contemporary political situation. In this case, the defendant leaked details of the Secretary of Justice Secretary's medical record to two local newspapers and was prosecuted for unauthorized Internet access and fraud under the Computer Crime Ordinance 1993. He staged a 'public interest' defence, stating that he had wanted to expose the fact the government had not told the truth about a key government official (the Secretary of Justice) being admitted to hospital for emergency surgery. The defendant's aim was to expose the newly formed Hong Kong Special Administrative Region government. By showing that the government had not been entirely honest about a key government official, the defendant's actions chimed with wider fears about the openness and transparency of the post-1997 regime. At the time, there was heightened public anxiety about the openness of the new HKSAR administration.

The defendant was found guilty under the Computer Crime Ordinance 1993 of unauthorized access to an Internet account and acting dishonestly and was sentenced to six months imprisonment. However, the appeal court judge stated that, "*this is an exceptional case…I do think that in these peculiar circumstances, a term of six months' imprisonment is clearly manifestly excessive*".[399] The six-month sentence was reduced to 100 hours community service.

[398] Transcript 5 (HK): p.13.
[399] See HKSAR v Tsun Shui Lun-[1999] 2 HKC 547, Magistracy Appeal No 723 of 1998.

The circumstances surrounding this case were peculiar, as they suggested a political rather than a criminal motive. After being arrested, the defendant spent seven days in police custody before he appeared in the Magistrate's Court. However, the fact that the original sentence was over-turned shows that the courts can act as a check on the power of the state, even where the case seriously embarrasses the government.

In most cases, the courts appear to be punishing the crime with little regard to the status of the offender. However, in **Case 6** the status of the offender did come into play. This case involved a referral from the Transport Department to the police concerning suspicions that a third person was defrauding someone's Internet bank account. On a number of occasions, a cheque issued to the Transport Department had bounced just before the bank making the withdrawal tried to take the money from the defendant's bank account. In fact, the defendant (a police officer) was intentionally transfer the funds from his Internet bank account to another bank account just before the funds were withdrawn to cover the issued cheque, leaving insufficient funds to cover the cheque issued to the Transport Department.

In this case, however, instead of being prosecuted for a criminal offence, the defendant was dismissed following an internal police disciplinary tribunal. The tribunal found him guilty of misconduct. The officer sought a judicial review. However, the case was dismissed and the original decision of the disciplinary tribunal was upheld.

If no application for judicial review had been made, the case would never have reached the public domain. The matter would have been dealt with internally by the police and the general public would never have become aware of the officer's misconduct. In following this course of action, the police themselves did not uphold the principle that everyone is equal before the law. Had it not been for the judicial review application, the matter would have by-passed the legal system altogether. Therefore, it may be that other cases follow a similar route and added to the 'dark figures' on unreported and/or under-reported crime in Hong Kong.

Because this case was originally dealt with behind closed-doors in a tribunal, it has the potential to feed into public fears about the erosion of the rule of law by the public authorities in the wake of the 1997 transfer of sovereignty and Hong Kong's greater integration into the political structure of the mainland. Moreover, the public have had a longstanding public suspicion about the independence and fairness of police internal disciplinary tribunals.[400] However, the fact the defendant believed that judicial review would provide him with justice suggests that at least some people still believe in due process under the rule of law.

(ii) Prosecuting quite minor Internet crimes

One question examined earlier was whether the police bother to prosecute relatively trivial and low-value offences. In **Cases 1**, **3** and **8** the actual monetary value involved was either low or zero. Even so, the defendant in **Case 1** received a six month custodial sentence. In **Case 3**, the defendant was sentenced to a detention centre, even though the monetary value of the crime was less than

[400] See Lam Siu Po v Commissioner of Police, Court of Final Appeal [2009] HKCFA 24. This police dismissal was quashed on appeal. The case highlighted the fact that the police disciplinary tribunal was unfair and biased toward the police.

HK$290. In **Case 8**, the defendant who earned bonus points was fined HK$5,000. Although these are all relatively trivial cases, they would have taken valuable time and resources to investigate.

(iii) Mainlandisation

Seven of the 15 cases involved transactions with mainland China. The majority of these cases involved large sums of money or were serious in other ways, such as corruption. In one case, **Case 13,** the corrupt mainland official identified in the case was beyond the reach of Hong Kong law. In cases such as this, corrupt mainland officials are dealt with not by the law but by internal party mechanisms. For example, in 2003, Liu Jinbao,[401] the former head of the Bank of China in Hong Kong, faced charges in relation to irregular loans in China. He was recalled to Beijing and disciplined internally by the Communist Party for his shortcomings.

(iv) Equal application of the law

The cases in the sample suggest that 'small fry' are prosecuted to the full extent of the law in Hong Kong as much as the 'big fry'. In other words, the police pursue all cases of banking fraud regardless of whether large or small amounts are involved, and the legislation is framed in such a way that it allows them to do so. The police also seem to be using the Computer Crimes Ordinance 1993 as 'catch all', at least at the start of an investigation, before switching to other, often more serious charges later. It is easier for the police to build a stronger case after

[401] See Bloomberg Business Week, (June 19, 2003) 'The Bank of China's Real Scandal'. Website: <http://www.businessweek.com/stories/2003-06-19/the-bank-of-chinas-real-scandal>. [Visited 27/6/2013].

the initial charges have been laid. For example, in Case **1**, a criminal law was used to prosecute a political act, which raises the question of the use the law as a pre-text for political policing.

The fact that the police will even prosecute minor offences was confirmed by a Chief Inspector interviewed for this research who said:

> "*Unlike other countries, other law enforcement agencies around the world, we do not set a minimum bar to take up the computer investigation, in terms of the monetary values etc… because investigation of the computer crime to HK police is still at a learning curve. So, even though the monetary value involved in a crime may be very low, we look at it as sort of learning process that our officer gains from it.*"[402]

However, an e-banker interviewed for this research said his impression was that the police only seek to prosecute high profile cases:-

> "*...so far they have sought high profile cases…like the one that was discussed at the AmCham seminar…but those are very individual case. I am not so sure whether the legal system or the prosecution in Hong Kong…like is sufficient enough to tackle this kind of case… but so far, there were some… like, more high profile cases exposed in Hong Kong…*"[403]

Nonetheless, the minor offences prosecuted in the case studies may be taken as evidence that the rule of law is being equally applied. For example, the youth who manipulated the Internet to gain bonus points in a casino game was prosecuted with the same vigour as the senior managers of Sin Hua Bank. However, in addition to supporting the idea that everybody is equal before the law, these cases suggest that the police in Hong Kong take a tough approach to crime-control and pursue everyone equally harshly. Accordingly, all offenders

[402] Transcript 8 (HK): p.1.
[403] Transcript 9 (HK): p.3.

are likely to receive a custodial sentence even for minor crimes. In this sense, the Hong Kong criminal justice system[404] leans towards 'crime control', in favour of the prosecution rather than the defendant. This stance was modified with the establishment of the Bill of Rights in 1991. Between 1991 and 1997, the Bill of Rights made crime control secondary to due process. However, after the transfer of sovereignty in 1997, the Basic Law became the most important constitutional law document,[405] overarching the national law of Hong Kong. Moreover, one of the requirements of the Basic Law is that Hong Kong must maintain its economic and political stability. Therefore, the 'crime control' approach to policing apparent in the case samples may reflect an attempt to protect Hong Kong's reputation as a 'clean' economy.

(v) Technological and Financial Knowhow 'Savviness'

A number of the defendants in the sample cases demonstrated a high level of technological and financial knowledge in conducting their crimes and exploiting new opportunities for gain. **Case 8,** for example, shows that this knowhow 'savviness' is evident among ordinary youth as much as the commercial elite.

[404] The Tiananmen Square incident in 1989 led to the introduction of the Bill of Rights (BoR) in 1991. Before that there was a tradition in the law of the presumption of guilt for a number of offences. The Police and Criminal Evidence Act 1984 'PACE', is a code of practice that established the powers of the police to combat crimes while protecting the rights of the public. PACE set out the balance between the powers of the police and the rights and freedoms of the public.

[405] See Basic Law instrument 9, which states, "*The Basic Law of the Hong Kong Special Administrative Region is constitutional as it is enacted in accordance with the Constitution of the People's Republic of China and in the light of the specific conditions of Hong Kong. The systems, policies and laws to be instituted after the establishment of the Hong Kong Special Administrative Region shall be based on the Basic Law of the Hong Kong Special Administrative Region*". Website: <http://www.basiclaw.gov.hk/en/basiclawtext/images/basiclawtext_doc9.pdf>, [Visited 22/6/2013].

(vi) Police Capability

A number of the officers interviewed for this thesis stressed that the police were well trained and highly capable in investigating Internet banking fraud. Several also emphasised the fact the police liaised with ISPs, the Department of Justice and banks in collected:

> "*We [the police] have regularly scheduled meeting with the DoJ and ISPs to discuss various issues about computer related crimes in Hong Kong, including the current trend in computer related crimes, offender methods, both new and old methods. The discussions would also involve how, and in what way, the ISPs can improve their side or the way of doing things, so that it can help the police to solve computer related crimes more quickly.*"[406]

**Case 7** reflects the capability of the Hong Kong police in investigating banking crime. In this case of Internet money laundering, bank transfers were made between Hong Kong, Taiwan and South Korea. This international case also threatened Hong Kong's financial reputation. Nonetheless, the TCD was able to liaise with agencies in the other jurisdictions and together they successfully traced the computer evidence across several countries.

This kind of international liaison is part of the Hong Kong police's strategy for tackling Internet crime. As the head of the TCD stated in an interview for this thesis, "*we are up to our capability, in the sense of handling existing technology crime, i.e. hacking, website defacing, online deception and fraud*".[407] He also commented that, "*since 2001, the Hong Kong police have been sent off to*

[406] Transcript 6 (HK): p.5.
[407] Transcript 7 (HK): p.14.

*mainland China, to assist…*".[408] Another respondent, a Manager of e-banking in a global bank said:

> "… it *is a borderless world, and it's hard to find you. It's easy to extract funds from an account and then lose your audit trails…I mean these guys are pros. They know what they're doing…the nature of crimes committed over the Internet is different from crimes committed offline in the real world. It's harder to detect where a criminal is located. For example, if they live, reside, in a different jurisdiction, there're jurisdictional issues whether the local police will investigate… So, there is an international aspect to have co-operation between international police…is up to the policing bodies to work together to try to tackle this area…*"[409]

The cases in this sample suggest that the police do have the capacity to conduct international investigations.

(vii) Bank/Police Liaison

The banks and the police both claim to liaise closely when it comes to Internet crime. As one respondent, a chief inspector in the TCD, stated, "*HK is a very small place, unlike the UK or US. It is quite easy for people to get together for meeting and exchange intelligence*".[410] However, an e-banker interviewed for this research argued that:

> "*the bank and the police like having very little communication, so on this kind of like computer crime situation, what we have done is, like, do it by ourselves, try to make our system as safe as possible… like, defend against the outside intruder…like, a strong security culture among our staff… try to make ourselves as safe as possible… So that is more standalone basis… a 'do it ourselves' attitude.*"[411]

[408] Transcript 7 (HK): p.5.
[409] Transcript 3 (HK): p.10.
[410] Transcript 8 (HK): p.11.
[411] Transcript 9 (HK): p.6.

Another respondent, a regional director for security of global credit card company also thought that bank/police liaison was not always as close as it seems:

> "*I can say this is very rare. The private sector people attend the regular meetings with the police discussing fraud cases … Certainly there are some exceptional cases, where they need to receive assistance.*"[412]

Opinion thus seems mixed as to whether the police and the banks work closely together. However, the case samples do provide evidence that the police and the banks do have a close working relationship. For example, in **Cases 12** and **15,** the prosecution called employees from the HSBC as expert witnesses. This kind of liaison confirms the link between the criminal justice system and the banks, and the finding that the bank staff provide forensic evidence for the prosecution. **Case 11** also showed that the HKMA co-operated closely with the SFC to monitor and refer a case for prosecution. The head of the TCD mentioned this close cooperation between the banks and law enforcement agencies in his interview. The manager of Internet banking at the HSBC also confirmed that she and her organisation regularly dialogue with the police on matters relating to Internet security. However, she also added that the discussions were not face-to-face talks with the police, because "*We have a dedicated unit to do that…we co-operate because it is necessary…We have that two-way channel.*"[413] She went on to explain that, "*our security division is made up of ex-policemen… we work with the police, we like to maintain a close working relation with them…*"[414]

[412] Transcript 10 (HK): p.5.
[413] Transcript 3 (HK): p.6.
[414] Transcript 3 (HK): p.7.

Summary

On the issue of whether the banks and the police closely liaise with one another in investigating and prosecuting Internet banking fraud, the evidence from the interview data is more mixed than that from the case sample, which seems to show a close liaison. There is also strong evidence from the sample cases that the police are capable of successfully investigating Internet banking fraud, even when the crimes are trans-jurisdictional. However, the police may have some problems when the cases involve mainland Communist Party officials, as these figures 'official' tend to be beyond the reach of Hong Kong police and law may not be able to reach them.

The sample cases also suggest that the police use the Computer Crimes Ordinance 1993 as a 'catch all' to initiate investigations, but then change the charges to traditional crimes at trial. There is also clear evidence in the sample cases to suggest that the police prosecute minor cases (i.e. trivial, low monetary value crimes) and cases involving 'big fish' (i.e. serious, high monetary value crimes).

Furthermore, there is some evidence that mainlandisation is influencing Internet banking crime in Hong Kong, as many of the cases involve mainland parties, and parties travelling to mainland China to do business. Some of the cases involved corruption, while others used the Internet in mainland China to perpetuate crimes in Hong Kong. As these cases suggest that mainland practices are seeping into Hong Kong, these types of crime may give rise to the fear that Hong Kong's

reputation as an international financial centre could be damaged if such practices go unchecked.

In addition, the high number of appeal cases in the sample and the judicial review suggest that the ideology of the rule of law is alive and well in Hong Kong. However, the high number of custodial sentences in the sample and the prosecution of minor crimes also suggest that the Hong Kong police use the law for the purposes of crime control rather than due process.

# Chapter Ten
# Conclusion

According to Wilbur Miller,[415] police practice in a particular place is shaped by a host of factors, including a society's history, law, socio-cultural and socio-economic conditions and its tradition of criminal justice. Because of these factors, 'policing' can differ between places, even when the police forces and legal frameworks in two places share similarity in policing origin and framework, as well as their laws.

Although Miller was discussing the policing in New York City policing and that city's place as a frontier city on the East coast of America in the nineteenth century, his approach remains relevant to the study of policing in other societies. Hong Kong is also a 'frontier city', in the sense that it was bordered by mainland China throughout the more than 150 years of its colonial rule. Moreover, Hong Kong remains a Special Administrative Region, which is not entirely unified socially, politically or legally with the mainland. Crime operates across this frontier, as was the case in nineteenth century New York, although these days this includes Internet crimes. Hong Kong has also long acted as an economic frontier town for economic migrants from southern China. Today, Hong Kong is also major migration hub for South East Asia and beyond, just as the Californian gold rush acted as a pull for migrants in the early nineteenth century America. In the 1990s, violent cross-border crime was an issue (such as kidnapping and armed gold-shop robberies); today the problem includes cross-border Internet crime.

[415] See Miller, W.R. (1973) (2nd Edition) Cops and Bobbies: Police Authority in New York and London, 1830-1970. Ohio State University Press: Columbus.

Miller's theory is useful for understanding Hong Kong policing in term of the society's history, law, and socio-cultural and socio-economic conditions, and its tradition of criminal justice. In this thesis, I have examined whether and how the 'policing' of a particular kind of economic crime in Hong Kong, namely Internet banking fraud, has been shaped by factors such as Hong Kong's distinctive history, policing tradition, laws, economic character and semi-authoritarian political structure, and the prevailing socio-cultural attitudes towards money and new technology. I have used interview data and case studies to uncover evidence on whether these factors have shaped how the banks, police and courts in Hong Kong 'police' Internet banking fraud.

Hong Kong's Economy

I have argued that Internet economic crime is high on the list of policing priorities in Hong Kong. Since the 1990s, the resources put into fighting economic crimes such as Internet banking fraud have risen significantly. As Wilding and Mok state:

> "*The bedrock of the Hong Kong government is to maintain a highly-rated economy by creating a favourable environment for foreign investment and international trade. The government believes that economic development is the basis of social development*".[416]

To retain Hong Kong's ranking as one of the world's top business centres[417] (Hong Kong is the fourth largest financial market in the world)[418] and to attract

[416] Wilding, P., Mok, K.H. (1997) 'Conclusion: Coming to a Judgement', in Wilding, P., Huque, A.S. and Tao Lai, P.W.J. (Eds.) Social Policy in Hong Kong. Cheltenham: Edward Elgar, p. 155.
[417] Tucker, S. (Monday, June 9 2008) 'Singapore Steals Marches on Hong Kong in Asia Battle', London: Financial Times Newspaper, p. 6.

international commerce, government policy has been geared towards providing economic stability and a good legal framework.[419] Despite its reputation for laissez-faire, ever since the early colonial years the Hong Kong government has actively tried to create the right environment for the economy to grow. The policing of economic crime is part of this environment. Because the government is executive led, it does not answer to the general public through the ballot box. Since the 1997 hand-over, the government has also been criticised as being a government of business for business. Therefore, if the government thinks that economic crimes such as Internet banking fraud are harmful to the economy, then policing receives the resources to place economic crime high on the list of policing priorities. The interview data presented in this thesis stress that the Hong Kong police are highly capable in policing this type of crime, and all the data point to major investments in police time, personnel, equipment and up-skilling. The expertise of the police complements that possessed by the banking sector, with which the police often liaise.

Culture

I have argued that because Hong Kong is a technologically and financially advanced society, Internet banking crime is more likely to occur. Most people regularly use the Internet for everyday personal banking and for dealing in stocks and shares. For many, watching the Internet for signs of movement in the market is a daily routine. Even ordinary youth have enough financial and technological

[418] Yiu, E. (Tuesday, September 2007) 'Trading Up'. Hong Kong: The South China Morning Post Newspaper, p.A19. In September 2007, there were 1,206 companies listed in the Hong Kong stock exchange and market capitalization is worth HK$19.6 trillion.
[419] Ibid. From stamp duty tax alone, in 2006, the government collected HK$15 billion from stock transactions.

knowhow to commit Internet crimes, as is shown by the case data. As the police are recruited from this population, they tend to already possess high-levels of technological and financial competence when they join the force.

What is the evidence as to how this affects the incidence, reporting and recording of Internet banking crime in Hong Kong? The existence of well-resourced specialist units within the police should mean that the police are able to recognise and prosecute the majority of cases of Internet banking fraud in Hong Kong. However, although the police have also made it easier for victims to report Internet crimes, and have trained their frontline officers to deal with the victims' reports, relatively few incidents of Internet banking fraud are reported in Hong Kong. As discussed in Chapter One, Wong suggests that there is a large dark figure of unreported crime in this area.

One possible reason for the low rates of reported Internet banking crime is that the public are simply reluctant to report crime at all, especially if the amounts involved seem small or the likelihood of catching the offenders seems low. Another possibility is that people are aware of the problem of Internet crime and take steps to avoid becoming a victim. Of course, the low number of reported crimes may also be due to the fact the victims do not realise they have been defrauded, although this seemed to be less likely for businesses and banks.

Furthermore, the crime statistics reflect the cases where an offender has been *charged*. The decision to prosecute a crime lies with the Department of Justice, which has its own thresholds and prosecution criteria. These criteria include a

stipulation that the cases that go to trial should more likely than not result in a conviction. Because of the complex nature of some of the evidence in Internet banking frauds, the prosecution may decide to pursue other charges that are easier to prove. Moreover, Internet banking fraud can be costly to pursue, which may also affect how a case is prosecuted. However, the case sample suggests that the use of public money is not always a factor, as the Department of Justice appears to be willing to prosecute and seek custodial sentences even in trivial cases.

The fact the statistics suggest that very few cases of Internet banking fraud are prosecuted may say more about how the police and prosecution choose to charge such cases, rather than their actual incidence of the crimes. The low levels of recorded Internet banking fraud probably also reflect the fact that during the course of investigations, crimes originally charged under the Computer Crimes Ordinance often get prosecuted as other, traditional types of crime. The sample cases clearly show that the charges change in this way during the course of the investigation. Thus, what starts out as a computer-related offence, does not always end up as one at trial, and therefore will not appear in the crime figures as such.

Another factor affecting the reporting and recording of Internet banking fraud is the banks themselves. The regulations expressly state that the banks must report any instances of such crimes to the authorities. The interview data and the case sample also show that the banks, police, HKMA, SFC and ICAC all operate in a co-ordinated manner to prevent, detect, investigate and prosecute Internet economic crimes. The law enforcement agencies regularly meet with each other

and the banks, and assist each other in investigating and prosecuting Internet banking crimes (for instance, by providing evidence in court cases).

However, the interview data show that the banks do not always report the instances of Internet banking fraud they detect to the authorities. Some of the interviewees stated that the banks would do so only as a last resort, to avoid risking their reputation, among other reasons. Some banks (such as small local banks) are also less equipped than others (such as large, international banks) to detect, investigate and report such crimes. The bigger banks tend to be the most capable because they possess the systems, resources and expertise to pursue complex and lengthy international investigations across the world. Equally, however, this also means that they are more able 'go it alone' when investigating Internet banking fraud, only contacting the police during the latter stages of the process when a case requires criminal prosecution. Both large and small banks may, however, prefer to sort out such matters by alternative means. Alternatively, both can become involved with the criminal justice system indirectly, as a result of police, SFC, ICAC and HKMA investigations into other types of crime that turn out to have an Internet banking fraud element.

The legal environment and rule of law

The law in Hong Kong has a significant effect on how cases of Internet banking fraud are charged and prosecuted. For instance, the Computer Crimes Ordinance 1993 (CCO) allows the police to charge offenders with computer crime offences, which then become traditional crimes, such as theft, corruption or handling stolen goods, later in the legal process. The ordinance is sufficiently flexible to allow

the police to use it as ‘catch all’, i.e. as a starting point for an investigation that might lead elsewhere and which allows the police to search for evidence of other crimes. The case sample clearly demonstrates that cases that were initially charged under the Computer Crimes Ordinance were later prosecuted as other types of crime.

Another important characteristic of the environment in which these cases occur is the rule of law, which holds that everyone is equal before the law. However, as discussed in Chapter One, a number of cases since 1997 have raised doubts about whether the rule of law is as strong as it was before 1997. The rule of law is one of Hong Kong’s core values. Everyone is supposed to be equal before and subject to the same law, and; no-one is liable to be punished unless they have broken the law.

The interview and case sample data provide some evidence to support the argument that at one level, the rule of law in Hong Kong is alive and well. For example, the large number of cases that went to appeal and/or judicial review suggests that the defendants still believed in the rule of law amongst, as they made full use of their due process rights. In addition, the case sample suggests there is equality before the law, as ‘big fish’ are just as likely to be prosecuted as ‘small fry’.

Moreover, at sentencing, all of the defendants were treated equally harshly by the courts. The case sample clearly shows that when these cases *do* come to trial, they are highly likely to end in conviction and a custodial sentence. This was true

for twelve out of the fifteen cases in the sample, and was the case in minor cases and cases of low monetary value. This suggests that the cases that do get to trial have been thoroughly investigated. It also suggests that the courts take a hard-line approach to Internet economic crime to protect Hong Kong's international reputation and the integrity of the financial system. In **Case 11,** for example, the judge explicitly stated that a viable electronic banking system and a clean stock market were vital to Hong Kong and that insider dealing would be severely punished. In **Case 7,** the judge also emphasised the harm that such crimes cause to Hong Kong's status as a financial and banking centre. In another case, *HKSAR v Mak Shing,* the judge again stated that Hong Kong's international reputation "*is not to be sullied*".

Mainlandisation

In Chapter One, I argued that the mainlandisation of Hong Kong since 1997 may have affected the nature of Internet economic crime and the way it is handled by the police. In this thesis, mainlandisation is defined as:

> *"[The] policy of making Hong Kong politically more dependent on Beijing, economically more reliant on the Mainland's support, socially more patriotic toward the motherland, and legally more reliant on the interpretation of the Basic Law by the PRC National People's Congress*."[420]

Since 1997, many in Hong Kong have feared that greater economic integration with mainland China will corrode the rule of law and Hong Kong's 'clean' status as an international financial centre. It is feared that the 'mainland ways of doing things' (such as corruption and the use of *guanxi*) will creep into Hong Kong

[420] See Chapter One

society. It is also feared that increased mainlandisation will lead to an influx of criminals and the breakdown of law and order, including e-crimes. Since 1997, the police have increasingly had to extend their investigations to mainland China, where the legal and political processes are very different to Hong Kong. In mainland China, the operation of both the police and the courts is closely tied to the Communist Party's political agenda, and the police and the courts must strictly toe the Chinese Communist Party line. They are not independent. As Lo states:

> "*… the CCP is the representative of the people. All the people's machineries, or state machineries, including the judiciary, are actually controlled by the CCP. Rule by the people is in fact "rule by the CCP". Thus, the judiciary is not absolutely independent and its decisions are always shaped by political considerations. Although China's Constitution ensures the independence of the court, in practice, the court is a "people's court," and thus, it has to literally toe the party line*."[421]

This connection with the political machinery in mainland China may mean that when the Hong Kong police seek assistance in collecting evidence in an Internet banking case, the mainland courts may take a different view of the offence. Economic information is also sometimes classified as a 'state secret' and cannot be divulged. To do so could result in detention and prosecution.

However, the government in Beijing is very keen to maintain Hong Kong's economic value to the mainland, and is also keen to crack down on corruption at home. As a result, it may in fact encourage mainland law enforcement agencies to cooperate with their Hong Kong counterparts in the fight against economic crimes. Either way, mainlandisation is likely to have an increasing influence on

[421] T. Wing Lo. (2012) Op. Cit.: p. 635.

the nature of Internet economic crime and the way it is handling by the criminal justice system.

The Hong Kong police do liaise with the mainland policing authorities in investigating Internet banking crime. The two sides exchange intelligence, mount join operations, help secure the evidence and co-operate with other international agencies in trans-jurisdictional crimes.

However, one case in the sample involving a corrupt mainland official showed that it can be difficult for the police to prosecute party members, as only the Hong Kong perpetrators were brought to trial in this case. The existence of this type of 'mainland factor' may contribute to the public's fears that mainlandisation is undermining Hong Kong's economy and the rule of law.

Other data also show that mainlandisation is having an effect on the nature and level of Internet banking crime. At least one of the police respondents and one Internet banker took the view that this type of cross-border economic e-crime was increasing. However, there are as yet no firm official data on whether mainlandisation has led to increase Internet banking fraud. The case samples also show that mainlandisation was a factor in many of the crimes. Seven out of the fifteen appeal cases involved a mainland factor, with either the victim or the perpetrator being situated in the mainland, or the case involving transactions between Hong Kong and mainland China businesses.

Bank Regulations

The HKMA was established by the government to regulate the banks. It licences all the banks in Hong Kong, and its licencing requirements are strict and tightly regulated. These tight external controls on the banks are connected to (i) the banking business environment and (ii) the history of the various banking scandals in Hong Kong. Although Hong Kong introduced its first banking laws in 1948 to control the banking industry, these laws were very liberal when compared with today's standards. This early liberal approach reflecting (as Miller might argue) Hong Kong's history as a trading port, and the belief in the principle of laissez-faire.

However, after a series of banking problems in the 1930s, 1950s, 1960s, 1970s, 1980s and early 1990s, the government and the banks called for tighter regulations. The government then established the HKMA as a statutory body to oversee the industry, because when the banks collapsed, there was a ripple effect and everybody in Hong Kong's financially-savvy society, from ordinary citizens, to business elites and international banking organisations. Riots as a result of the BCCI collapse, for example, threatened social and political stability Again, in September 2008, there was a rumour that the Bank of East Asia might collapse. The New York Times reported that:

> "*Smaller depositors were rushing to retrieve their money, On Wednesday afternoon, about 200 people lined up outside a branch of the Bank of East Asia in eastern Hong Kong, forming a line that snaked around the block. Bank executives walked up and down the crowd, handing out statements denying it was in trouble.*"[422]

[422] New York Times (24th September 2008), "Rumors prompt run on Hong Kong bank". [Online] [Cited 28/07/2009] <http://www.nytimes.com/2008/09/24/business/worldbusiness/24iht-

Everyone, from grandmothers and taxi drivers, to housewives and veteran investors battled for a place in the queue to try to retrieve their money. Similarly, in the early 1990s, the collapse of the Bank for Credit and Commerce International (BCCI) had a similar impact, leading to the threat of riots.[423] The Hong Kong government refused to rescue BCCI and the bank collapsed, leaving almost 40,000 depositors high and dry. Some depositors wept on the street, some went on hunger strike, while others organised protest marches. The collapse of BCCI also triggered a massive bank run, which sent the Hang Seng Index into a nosedive. In the end, to stabilise the situation, the government moved to inject massive public funds into the Hong Kong banking system.[424] This response reflects the importance of the banking sector to society, economy and polity of Hong Kong.

Political Environment

I have also argued that the way a society is policed, in this case the way Internet banking fraud is policed, is affected by that society's political structure. Loader and Walker argue that a key feature of policing in an authoritarian state such as

---

24asiabank.16438911.html>. See fuller discussion in Roebuck, D. (ed.) (1994) Law relating to banking in Hong Kong, (2nd Edition). Hong Kong: Hong Kong University Press, pp. 307-320.

[423] In the 1960s, social instability and violence shook the foundations of Hong Kong. The property market plummeted and people took their cash and left for other countries, such as the US and Australia. More recently, a similar capital flight occurred in the early 1990s, in the aftermath of the Tiananmen Square incident on June 4th 1989. In Hong Kong, property prices fell and the value of stocks and shares plummeted. As Bumgarner and Prime argued: "*Owing largely to the uncertainty surrounding Hong Kong and China, many Hong Kong investors chose to move their capital out of Hong Kong. This capital flight changed the investment environment in places, such as Vancouver, British Columbia, Canada…Many of the Hong Kong Chinese who have settled in Vancouver invested billions of dollars in the local economy, between 1994 and 1996. Estimates of the loss of Hong Kong assets to Canada and other destinations are as large as US$75 billion*". Bumgarner, M.K., Prime, P.B. (2000) 'Capital mobility and investor confidence: The case of Hong Kong's reversion to China's sovereignty'. Pacific Economic Review. Vol. 5, Issue 2, p. 270.

[424] See fuller discussion in Roebuck, D. (ed.) (1994) Law relating to banking in Hong Kong, (2nd Edition). Hong Kong: Hong Kong University Press, pp. 307-320.

Hong Kong is the protection of the interests and ideology of the regime, and of the private interests that it supports and that support it.[425] Hong Kong is not a democratic society, and never has been. It is a semi-authoritarian city state and an 'economic city', where the business elite and the government share common ground in protecting the economy. Accordingly, the people who dominate policy making in the Hong Kong government are largely prominent merchants and professionals. As a reflection of this, two out of the Commissioner of Police's seven operational priorities are related to economic crimes, one of which is technology related crime. Moreover, China is aware that Hong Kong is a leading international financial centre in Asia. Its 'mini-constitution' for post-1997 Hong Kong, the Basic Law, specifies that the Hong Kong government must maintain the region's status as an international financial centre. According to Article 109, "*The Government of the Hong Kong Special Administrative Region shall provide an appropriate economic and legal environment for the maintenance of the status of Hong Kong as an international financial centre*".[426]

The post-1997 'government by tycoons for tycoons' coincided with a major investment in resources for the policing of high-tech economic Internet crime. This was described by respondents in interview. However, one of the weaknesses of a non-democratic society is that when things go wrong (as in the above examples) the blame cannot be spread. Instead it goes straight to the top, to the government. Without a democracy, the only option left to Hong Kong people is to vote with their feet, by protesting on the street. Protests have increased since 1997, in July 2003 500,000 people protested in an anti-government

[425] Loader, I., Walker, N. (2007) Ibid.
[426] See Basic Law, Article 109.

demonstration. Despite promises that post-1997, 'Hong Kong people will rule Hong Kong', ordinary people have little say in who rules them. Moreover, during the early post-1997 period, the government was criticised for being a government of tycoons who ruled in their own interests.

As Lau argues[427], Hong Kong's reintegration with mainland China has complicated the government's relationship with the masses and its commercial elite supporters. As a result, Hong Kong has become more difficult to govern. Lau Siu Kai argues that when the Basic Law was drafted, it was deemed by Beijing to be the most appropriate political framework to allow Hong Kong to maintain its stability and prosperity after the end of colonial rule.[428] However, the Basic Law has given rise to inherent contradictions in Hong Kong's internal politics, and the coherence between the business elite and the state is no longer the same as it was under colonial rule. Lau asserts that the state of Hong Kong's political affairs is now inherently contradictory, with the differences among the elites, between the elites and the government, and the elites and popular masses increasing widening.[429] Chiu and Lui also claim that the blueprint for the institutional arrangements of post-colonial Hong Kong, which are deliberately preserved in the Basic Law, no longer fit the needs of the new era, due to the changes in the broader socio-economic and political environment.[430] They state that:

[427] See Lau Siu Kai, (2002) 'Hong Kong's Partial Democracy under Stress'. In Yue-man Young (ed.) New Challenges for Development and Modernization: Hong Kong and the Asia-Pacific Region in the New Millennium. Hong Kong: The Chinese University Press, p. 181.
[428] See Lau Siu Kai (2002) Op. Cit.: pp. 181-182.
[429] See Lau Siu Kai (2002) Op. Cit.: pp.183-198.
[430] See Chiu, S. Lui Tai-Lok (2009) Hong Kong: Becoming a Chinese global city. Abingdon: Routledge, p. 109.

> "*... Institutional incongruity is a critical factor in bringing about the governance crisis in post-colonial Hong Kong… Since the 1970s [Hong Kong] has witnessed rising popular demands for policy outputs and political participation, but the problem encountered by the SAR government is not simply that of demand overload from below... but equally significant is the political restructuring triggered by the long-term emergence of local Chinese capitalists and the more immediate process of decolonization. The resulting constitution and re-constitution of the dominant class has wider repercussions for state-society relations and the capacity of the SAR government to govern... In other words, the SAR government faces a challenge not only in meeting popular demands from below… It also faces a challenge in gaining the cooperation of resourceful and influential capitalists, who [are] uncertain whether and how their interests would be protected in the post-colonial era.*"[431]

In this sense, the 'zero tolerance' approach to Internet economic crime and the associated major investment in police capability partly reflects the post-1997 government's need to reassure the business elite that their interests would be protected. This move formed part of a wider initiative in the early 2000s to're-invent' post-1997 Hong Kong as 'Asia's World City'. Other parts of this initiative included building the 'Cyberport' and the investment in new technology.

However, Lau, argues that it is not as simple as it once was to argue that the interests of the government and those of the business elite are one and the same. Lau has called for:

> *"The formation of a strategic governing alliance for the purposes of maintaining effective governance after the 1997 handover… The viability of ... an executive-led polity depends on obtaining reliable and steady support from a powerful and influential governing alliance ...*

[431] Chiu, S. Lui Tai-Lok (2009), pp.109-110.

> *This alliance is also expected to be able to reach out and secure grassroots support… the absence of support from a powerful strategic governing alliance will in the long run not only jeopardize the effectiveness of the SAR government's rule, but will also undermine the rationality and legitimacy of the entire political system".*[432]

This means that the investment in the high-tech policing of economic crime may not only reflect the interests of the business elite, but also the need of the government to secure grass-roots support. This means reassuring small, everyday investors and big tycoons alike that their money is safe when using Internet banking. This reassurance is required to preserve the government's political legitimacy and social stability. This would also chime with Hong Kong's image as a city of international finance, as a place where money is a central part of the local culture and as a city which has, in the past, witnessed disturbances because of financial instability. Therefore, the policing of Internet banking fraud and other kinds of economic crime affects the everyday lives of the masses as much as the fortunes of tycoons.

[432] Lau Siu Kai, cited in Chiu, S. Lui Tai-Lok (2009), p. 108